



Utilisation des réseaux de capteurs de canne pour les applications de surveillance de personnes

Sabri Khssibi

► To cite this version:

Sabri Khssibi. Utilisation des réseaux de capteurs de canne pour les applications de surveillance de personnes. Ordinateur et société [cs.CY]. Université Toulouse le Mirail - Toulouse II; Université de la Manouba (Tunisie), 2015. Français. NNT : 2015TOU20078 . tel-01331022

HAL Id: tel-01331022

<https://theses.hal.science/tel-01331022>

Submitted on 13 Jun 2016

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



THÈSE

En vue de l'obtention du

DOCTORAT DE L'UNIVERSITÉ DE TOULOUSE

Délivré par :

Université Toulouse - Jean Jaurès

Cotutelle internationale avec "Ecole Nationale des sciences de l'informatique, Université de la Manouba, Tunisie "

Présentée et soutenue par :

Sabri KHSSIBI

le mardi 29 septembre 2015

Titre :

Utilisation des réseaux de capteurs de canne pour les applications de surveillance de personnes

École doctorale et discipline ou spécialité :

ED MITT : Domaine STIC : Réseaux, Télécoms, Systèmes et Architecture

Unité de recherche :

IRIT équipe IRT-Blagnac et CRISTAL équipe RAMSIS

Directeur/trice(s) de Thèse :

Pr. Thierry VAL

Pr. Leila AZZOUZ SAIDANE

Jury :

Pr. KACHOURI Abdennaceur, Rapporteur

Dr. GUITTON Alexandre, Rapporteur

Dr. VAN DEN BOSSCHE Adrien, Encadreur

Dr. IDOUDI Hanen, Encadreur

Dédicace

À ma mère **KAHLA**.

Que nulle dédicace ne puisse exprimer ce que je lui dois, pour sa bienveillance de plus jeune enfance, son affection, son soutien et ses prières, en témoignage de mon profond amour et ma grande reconnaissance.

À qui je dois ma réussite.

À mon père **Bader**.

Aucun mot ne serait témoigner de l'étendue des sentiments que j'éprouve à son égard.

À mon cher frère **Assahbi**.

À ma chère future épouse **Manel**.

À tous ceux qui m'aiment.

À tous ceux qui ne cessent de m'encourager.

À tous ceux qui ont confiance en moi.

Je dédie ce travail...

Sabri KHSSIBI

Remerciement

Cette thèse m'a permis de voyager, vivre et travailler de part et d'autre de la méditerranée ce qui fut une aventure formidablement enrichissante à tous points de vue. Cette organisation m'a permis de profiter des compétences et de l'expérience de nombreuses personnes. La thèse ne peut être menée sans le soutien et la confiance d'un grand nombre de personnes. Je tiens à les remercier ici chaleureusement. J'en oublierai certainement quelques-unes et je les prie de m'en excuser par avance.

Je tiens d'abord à remercier mes co-directeurs de thèse, Monsieur **Thierry VAL** et Madame **Leila AZZOUZ SAIDANE** pour m'avoir permis de relever le défi de la cotutelle entre l'université de Toulouse Jean Jaurès, en France, et l'école nationale des sciences de l'informatique, en Tunisie.

Tous deux ont su diriger et orienter les travaux de recherche tout en me laissant suffisamment d'autonomie pour accomplir mon doctorat et apprendre la recherche. Ils ont tous deux, à leurs façons, manifesté un intérêt constant et constructif pour ce projet. Leur disponibilité et leur appui m'ont été bien utiles dans les moments les plus incertains et les plus pénibles.

Je remercie Madame **Hanen IDOUDI** et Monsieur **Adrien VAN DEN BOSSCHE**, mes deux co-encadreurs, pour leur soutien moral et leur disponibilité. Vos remarques ont été toujours pertinentes et précieuses. J'ai appris beaucoup de vous et vous m'avez guidé énormément.

Il était un honneur pour moi de travailler avec des encadrants et des directeurs de thèse comme vous, je vous remercie pour vos critiques, vos conseils très précis sur mes travaux de recherche et pour avoir relu, corrigé et commenté très soigneusement ce manuscrit.

Mes remerciements s'adressent également à Monsieur **Alexandre GUITTON** et Monsieur **Abdennaceur KACHOURI** qui me font l'honneur d'examiner et de rapporter sur ce mémoire. Merci pour le temps qu'ils ont pu consacrer à cette tâche et pour les remarques enrichissantes qu'ils ont formulé.

Je voudrais également remercier l'ensemble des membres des deux laboratoires qui, un jour ou l'autre, m'ont apporté une aide ou un conseil. Je leur souhaite bonne chance pour la fin de leur thèse, stage ou post-doctorat si ce n'est déjà fait.

Mention spéciale à mon frère **Assahbi** qui ne se défait jamais lorsque je lui demande de l'aide. Ta présence et ton aide morale ont été un élément crucial pour réaliser ce projet. Je voudrais te dire merci pour ton soutien pendant mes périodes de doutes et pour tes multiples encouragements répétés.

Je remercie ma chère épouse **Manel** pour son soutien et sa patience durant la période de préparation de ma thèse. Je la remercie énormément d’avoir été à mon écoute et surtout de m’avoir encouragé lors des quelques petits moments stressants de cette thèse. Comme tu me dis toujours : “le chemin est long, mais je sais que tu es là. Il faut s’accrocher jusqu’à la fin”.

Simple étant les plus forts, j’adresse toute mon affection à mes parents, et en particulier à ma maman **Kahla** qui m’a fait comprendre que la vie n’est pas faite que de problèmes qu’on pourrait résoudre grâce à des formules mathématiques et des algorithmes. Malgré mon éloignement depuis de nombreuses années, leur intelligence, leur confiance, leur tendresse, leur amour me portent et me guident tous les jours. Elle est la clef de ma réussite, sans elle à mes côtés, cette réalisation n’aurait pas la même saveur.

Je remercie mon père **Bader** qui m’a suivi dans ce long parcours étudiant et qui m’a beaucoup encouragé du début à la fin. Je vous remercie pour votre soutien moral et financier sans faille. Vos patiences et vos écoutes m’ont guidé énormément pour avoir les idées claires.

Merci pour avoir fait de moi ce que je suis aujourd’hui. Est-ce un bon endroit pour dire ce genre de choses ? Je n’en connais en tous cas pas de mauvais. Je vous aime.

Merci à tous!

Auteur : Sabri KHSSIBI

Titre : Utilisation des réseaux de capteurs de canne pour les applications de surveillance de personnes

Directeurs de la thèse : Thierry VAL et Leila AZZOUZ SAIDANE

Co-encadrants : Adrien VAN DEN BOSSCHE et Hanen IDOUDI

Lieu et date de soutenance : IUT-Blagnac, 29 septembre 2015

Résumé :

Le monde actuel connaît de profondes mutations démographiques étroitement liées au développement du domaine de la santé publique. L'accroissement de l'espérance de vie s'accompagne d'une augmentation du nombre des personnes âgées, en particulier celles atteintes de maladies chroniques. Plusieurs projets de recherche existants ont comme objectif d'assurer le maintien à domicile des personnes âgées, par un meilleur suivi en utilisant les nouvelles technologies. Parmi eux, nous trouvons le projet CANet qui propose l'utilisation de la canne comme un outil de surveillance non intrusif par l'intégration d'une multitude de capteurs. La canne utilise un système de communication sans fil qui lui permet d'échanger avec un centre de collecte ou de surveillance. Cette solution technologique permet le respect de la vie privée des personnes âgées, sans limiter leur liberté. Notre sujet de thèse s'inscrit dans le cadre de ce projet CANet. Les travaux de thèse sont principalement organisés autour de la conception d'une architecture topologique protocolaire, et des méthodes d'accès aux réseaux sans fil qui permettent la surveillance des personnes âgées à travers un réseau de capteurs embarqués dans une canne. L'objectif principal de la thèse est l'étude des architectures et des protocoles mis en œuvre au niveau communication sans fil pour offrir une infrastructure réseau fiable pour divers services de surveillance, de mesures et d'acheminement de données vers un centre de contrôle distant (cabinet médical, membres de la famille, etc.). Ces propositions ont fait l'objet d'une étude théorique et d'analyses de performances par simulation.

Mots clés : MAC, IEEE802.15.4, QoS, E-santé, Différenciation, Réseaux de capteurs sans fil, simulation

Discipline : Réseaux, Télécoms, Systèmes et Architecture

Laboratoires :

- IRIT équipe IRT-Blagnac Toulouse, France
- CRISTAL équipe RAMSIS, Tunisie

Author: Sabri KHSSIBI

Title: Using cane sensor networks for people monitoring applications

Thesis advisors: Thierry VAL and Leila AZZOUZ SAIDANE

Supervisors: Adrien VAN DEN BOSSCHE and Hanen IDOUDI

Place and defense date: IUT-Blagnac, september 25, 2015

Abstract:

The world today is undergoing profound demographic changes closely linked to the development in the health field. The increase in life expectancy was accompanied by an increase in the number of elderly people. Especially, those with chronic diseases. Many new research projects propose the use of the new technologies to provide home care of the elderly. Among them, we find the CANet project, which proposes the use of the cane as a non-intrusive monitoring tool through the integration of a multitude of sensors. The cane uses a wireless communication system that allows it to interact with a collection center or monitoring. This technological solution enables the respect of the private life of older people, without limiting their freedom. Our thesis is a part of the CANet project. The thesis work is mainly organized around the design of a protocol topological architecture, and methods of access to wireless networks that allow the monitoring of elderly people through a network of sensors embedded in a cane. The main aim of the thesis is the study of architectures and protocols implemented in wireless communication standard to provide reliable network infrastructure for various services monitoring, measurement, data routing to a remote control center (medical office, family members, etc.). These proposals have been the subject of a theoretical study and analysis of performance by simulation.

Key words: MAC, IEEE802.15.4, QoS, E-health, Différenciation, WSN, Simulation

Discipline: Networks, Telecommunications, Systems and Architecture

Laboratories:

- IRIT team IRT-Blagnac Toulouse, France
- CRISTAL team RAMSIS, Tunisia

Table des matières

Table des matières	vi
Table des figures	ix
Liste des tableaux	xii
Glossaire	xiii
Introduction générale	1
1 Contexte et motivation	1
2 Problématique	3
3 Contribution de la thèse	4
4 Structure du rapport	5
1 Systèmes d'aide aux personnes âgées et réseaux de communications adaptés	6
1.1 E-santé et applications	6
1.1.1 L'e-santé	6
1.1.2 Quelques applications de l'e-santé	8
1.1.2.1 Co-robo Cane : le robot qui vit dans la canne	8
1.1.2.2 THE AID : Une canne de gestion de santé personnelle	9
1.1.2.3 Canne intelligente : Le successeur réaliste de THE AID	9
1.1.2.4 Le projet CANet	9
1.1.2.5 FWD Powershot	10
1.1.2.6 Intelligent Racquet	10
1.1.2.7 Discussion	11
1.2 Technologies des réseaux sans fil	12
1.2.1 Analyse des architectures réseaux adaptées	12
1.2.2 Différentes technologies potentielles	13
1.2.2.1 De Bluetooth à BLE	14
1.2.2.1.1 Apparition de BLE	14
1.2.2.1.2 Couche physique et topologies de BLE	15
1.2.2.1.3 Pile protocolaire de BLE	17
1.2.2.1.4 Rôles définis pour le BLE	17
1.2.2.2 La norme IEEE 802.15.4-2006	20
1.2.2.2.1 Topologie d'un réseau IEEE 802.15.4	21
1.2.2.2.2 Modes de synchronisation de la norme IEEE 802.15.4	23

1.2.2.2.3	Couche physique de la norme IEEE 802.15.4 . . .	25
1.2.2.2.4	Amendements de IEEE 802.15.4	26
1.2.2.3	La norme IEEE 802.15.6-2012	27
1.2.2.3.1	Type de nœud et technologie physique	27
1.2.2.3.2	Topologies définies	29
1.2.2.3.3	Gestion du réseau	30
1.2.2.4	ANT : Advanced and adaptive Network Technology . . .	32
1.2.2.4.1	Notion de <i>Master</i> et <i>Slave</i>	33
1.2.2.4.2	Paramètres de connexion	34
1.2.2.4.3	Processus d'établissement de connexion	35
1.2.2.4.4	Couches supérieurs de ANT : ANT+	36
1.2.2.5	Discussion	37
1.3	Qualité de service dans la littérature	42
1.4	Conclusion	44
2	Contribution technologique et modélisation architecturale	46
2.1	Contexte et problématique	47
2.2	Profils de capteurs	49
2.2.1	Capteurs définis dans le projet CANet	49
2.2.2	Critères de classification	52
2.2.2.1	Périodicité des données	52
2.2.2.2	Débit nécessaire	53
2.2.2.3	Priorités	55
2.2.3	Classification des capteurs	56
2.3	Topologie globale proposée	60
2.3.1	Problématique spécifique	60
2.3.2	Topologie proposée	61
2.3.2.1	Niveau 1 : liens entre la canne et les capteurs du corps humain	62
2.3.2.2	Niveau 2 : liens directs entre cannes	63
2.3.2.3	Niveau 3 : liens entre cannes et PA	63
2.3.2.4	Niveau 4 : liens entre PA	64
2.3.2.5	Niveau 5 : lien avec un centre de collecte	65
2.3.3	Vue globale de la topologie choisie	65
2.3.4	Solutions technologiques proposées	66
2.3.5	Les limites de la solution proposée	68
2.4	Architecture protocolaire	69
2.4.1	Présentation détaillée de notre solution	69
2.4.2	Traitement des profils équivalents par la couche différenciation . .	72
2.4.3	Présentation des messages et des primitives associées	73
2.4.3.1	Messages de données	73
2.4.3.2	Message d'alerte	74
2.4.3.3	Messages de notification	75
2.4.3.4	Communication audio	77
2.4.3.5	Demande de libération de la période CAP suivante	80
2.4.4	Diagramme d'état	81
2.5	Etude théorique de BO et SO	82

2.5.1	Variation du débit en fonction de BO et SO	83
2.5.2	Choix des valeurs de BO et SO	85
2.6	Etude de la transmission de la voix	88
2.6.1	Choix du codec	88
2.6.2	Etude de la transmission de la voix	92
2.6.3	Algorithme de gestion de la transmission audio	95
2.6.4	Expérimentations	96
2.7	Conclusion	98
3	Evaluation des performances et modélisation	99
3.1	Choix du simulateur	99
3.2	Validation des valeurs de BO et SO	100
3.3	Etude par simulation de la couche de différenciation	104
3.3.1	Configuration réseau	105
3.3.1.1	Calcul du nombre de slots nécessaires pour la transmission	105
3.3.1.2	Calcul de la valeur BO et SO	105
3.3.2	Transmission dans les deux périodes de la même supertrame	106
3.3.2.1	Paramètres de simulation	107
3.3.2.2	Transmission dans l'une des deux périodes	108
3.3.3	Transmission dans les deux périodes CFP et CAP de la même supertrame	110
3.3.3.1	Transmission sans BER	110
3.3.3.2	Transmission avec $BER = 10^{-7}$	113
3.3.3.3	Explication du fonctionnement de la purge	116
3.3.3.4	Impact du BER	120
3.3.4	Présence d'une alerte dans le réseau	124
3.4	Bilan	129
3.5	Conclusion	130
	Conclusion générale et perspectives	131
1	Conclusion générale	131
2	Perspectives	134
	Publications personnelles	135
	Bibliographie	137

Table des figures

1.1	Comparaison entre les piles protocolaire de BLE et Bluetooth classique	14
1.2	Relation entre les différentes versions de Bluetooth	15
1.3	Différents rôles de BLE avec les fonctionnalités utilisées	18
1.4	Diagramme d'état des noeuds BLE <i>Broadcaster</i> et <i>Peripheral</i>	19
1.5	Diagramme d'état des noeuds BLE <i>Observer</i> et <i>Central</i>	19
1.6	Topologie en étoile	22
1.7	Topologie maillée	22
1.8	Topologie en arbre	22
1.9	Topologie générale complexe	22
1.10	Modes d'exécution de la sous-couche MAC de la norme IEEE 802.15.4-2006	23
1.11	Structure d'une supertrame	24
1.12	Les différents scénarii présentés dans la norme IEEE 802.15.6	28
1.13	Topologies utilisées dans la norme IEEE 802.15.6	29
1.14	Topologies recommandées par la norme IEEE 802.15.6	30
1.15	Composition de la supertrame dans le mode avec <i>beacon</i>	31
1.16	Les différents rôles joués par un nœud ANT	33
1.17	Les périodes de canal de ANT	35
1.18	La gestion de la direction de ANT	35
1.19	Pile protocolaire ANT/ANT+	36
1.20	Utilisation de BLE, Wifi et Zigbee dans les applications de maison intel- ligente et de Smartphone	38
1.21	Classification des algorithmes de QoS dans 802.15.4	43
2.1	Exemple des capteurs inclus dans la canne	47
2.2	Relation entre les capteurs corporels et la canne	62
2.3	Modélisation de la topologie canne-PA	64
2.4	Topologie maillée des PA	64
2.5	Topologie globale retenue	66
2.6	Relation entre les différentes technologies	67
2.7	La position de la sous-couche de différenciation	70
2.8	Composants de la couche différenciation	71
2.9	Séquence de transmission des messages	74
2.10	Traitement du message d'alerte	75
2.11	Cas d'un réseau dans l'état initial	76
2.12	Diagramme d'activité de calcul du Backoff	77
2.13	Initialisation de transmission de message de profil 4 côté canne (cas sans refus de la demande)	78
2.14	Demande de libération de la période CAP	80

2.15	Automate d'état de la couche différenciation	81
2.16	Débit moyen en fonction de BO et SO	83
2.17	Variation du superframe duration (SD) en fonction de BO et SO	84
2.18	Variation du superframe duration en fonction de SO et du débit moyen avec BO = 14	84
2.19	Variation de la durée inactive en fonction de BO et de BO - SO	85
2.20	Appel d'urgence	92
2.21	Réception d'un appel	92
2.22	Supertrame utilisée pour le cas 1	93
2.23	Supertrame utilisée pour le cas 2	94
2.24	Réservation des ressources pour la transmission audio	96
2.25	Etapes de transmission de voix	97
2.26	Transmission avec l'utilisation de codec Speex	97
2.27	Résultat du codec Opus avec un débit de 24.6 kbits/s	97
3.1	Pourcentage des messages reçus dans CFP avec BO = SO	101
3.2	Transmission des messages pour BO = SO = 0, 1 et 14	102
3.3	Période de transmission pour BO = SO = 14	102
3.4	Pourcentage des messages reçus dans la CAP avec BO = 14	103
3.5	Pourcentage des messages reçus	108
3.6	Nombre de messages non entrés dans la file FMT (avec conservation des trames qui seront transmises en CSMA/CA)	109
3.7	Nombre moyen de trames rejetées par la couche MAC après un échec de transmission)	109
3.8	Exemple de transmission	110
3.9	Taux de messages reçus dans la période GTS	111
3.10	Nombre moyen des messages reçus dans la période CAP	113
3.11	Taux de messages reçus dans la CAP avec $BER = 10^{-7}$	114
3.12	Délai moyen de bout en bout dans la CAP avec $BER = 10^{-7}$	115
3.13	Taux de messages reçus dans la CFP avec $BER = 10^{-7}$	116
3.14	Délai moyen de bout en bout des messages reçus dans la CFP avec $BER =$ 10^{-7}	116
3.15	Exemple de transmission sans l'utilisation de la purge	117
3.16	Exemple de transmission avec l'utilisation de la couche différenciation	118
3.17	Exemple de transmission avec l'utilisation de la purge	119
3.18	Suite de l'exemple présenté dans la figure 3.17	119
3.19	Pourcentage des trames en échec	120
3.20	Nombre moyen de trames rejetées par la file FMT avec $BER = 10^{-7}$	120
3.21	Nombre moyen de messages reçus dans la CAP	121
3.22	Nombre moyen de messages qui ne sont pas rentrés dans la file FMT	122
3.23	Différents cas de retransmission	122
3.24	Nombre moyen de trames rejetées par la sous-couche MAC à cause d'échecs de transmission	123
3.25	Nombre moyen de trames reçues dans la période CFP sans ACK	123
3.26	Nombre moyen de trames rejetées par la file FMT	123
3.27	Nombre de messages générés par l'application 1	125
3.28	Nombre de messages générés par l'application 2	126

3.29	Pourcentage des trames non acceptées par la file FMR	126
3.30	Pourcentage des messages non acceptés par la file FMR	126
3.31	Pourcentage de nombre moyen des messages reçus dans la CFP	127
3.32	Pourcentage de nombre moyen des messages reçus dans la CFP pour 7 noeuds	128
3.33	Longueur moyenne maximale de la file FMR pour 3 noeuds	128
3.34	Longueur moyenne maximale de la file FMR pour 7 noeuds	128
3.35	Nombre moyen d'essais de transmission pour 3 noeuds	129
3.36	Nombre moyen d'essais de transmission pour 7 noeuds	129

Liste des tableaux

1.1	Différents scénarii associés à des bandes de fréquences adéquates	28
1.2	Priorités associées à chaque type de trafic	32
1.3	Comparaison entre les 4 principales technologies étudiées	41
2.1	Capteurs proposés pour le projet <i>CANet</i>	51
2.2	Classification des capteurs en profils	58
2.3	Périodes de transmission associées à chaque profil	60
2.4	Primitives et messages nécessaires pour l'établissement d'une communi- cation vocale	79
2.5	Généralisation des paramètres des profils	87
2.6	Paramètres des codecs	89
2.7	Correspondance entre le codec et les valeurs de BO et SO	91
2.8	Valeur de SD	91
2.9	Information sur l'influence de la valeur de BO et SO	94
2.10	Les valeurs acceptables de BO et SO	94
3.1	Paramètres utilisés dans le premier scénario	101
3.2	Paramètres de la deuxième simulation	103
3.3	Paramètres des simulations	107
3.4	Paramètres des simulations	108
3.5	Paramètres des simulations	110
3.6	Paramètres du réseau pour une simulation d'alerte	125

Glossaire

ATT	A tttribute protocol
ANT	A dvanced and adaptive N etwork T echnology
AFH	A daptive F requency H opping
BAN	B ody A rea N etwork
BE	B ackoff E xponent
BI	B eacon I nterval
BLE	B luetooth L ow E nergy
BO	B eacon O rders
BPSK	B inary P hase- S hift K eys
BR	B asic R ate
CAP	C ontention A ccess P eriod
CACCA	C oexistence A ware C CA
CCA	C lear C hannel A ssessment
CMAP	C oordinator M esh A ccess P oint
CPL	C ourants P orteurs en L igne
CEN	C omité E uropéen de N ormalisation
CFP	C ontention F ree P eriod
codec	C ompression/ D ecompression M odule
CRC	C yclic R edundancy C heck
CSMA/CA	C arrier S ense M ultiple A ccess with C ollision A voidance
CSS	C hrip S pread S pectrum
CW	C ontention W indow
DTM	D ébit T héorique M oyen
DSSS	D irect S equence S pread S pectrum
EAP	E xclusive A ccess P hase
EDR	E nhanced D ata R ate
EHPAD	E tablishement d' H ébergement pour P ersonnes A gées D épendantes
EPS	E volved P acket S ystem
FFD	F ull F unction D evice
FMT	F ile des M essages T olérants
FM-UWB	F requency M odulated UWB
FMR	F ile des M essages temps R éel
FMU	F ile des M essages U rgents
GAP	G eneric A ccess P rofile

GATT	Generic Attribute Profile
GTS	Guaranteed Time Slot
HBC	Human Body Communication
HCI	Host Controller Interface
HL7	Health Level 7
HP	High Priority
HS	HeadSet
IEEE	Institute of Electrical and Electronics Engineers
IFS	InterFrame Spacing
IPV6	Internet Protocol Version 6
IR	Infrared
IR-UWB	Impulse Radio UWB
IrDa	Infrared Data Association
ISM	Industrial, Scientific and Medical
ISO	International Standardized Organization
GPS	Global Positioning System
LCD	Liquid Crystal Display
LP	Low Priority
LRP-UWB	Low RatePulse repetition frequency UWB
LIFS	Long InterFrame Spacing
LOS	Line Of Sight
L2CAP	Link layer Common AdaPtation layer
MAP	Managed Access Phase
MBAN	Medical Body Area Network
MICS	Medical Implant Communications Service
MSK	Minimum Shift Keying
MTU	Maximum Transmission Unit
NLOS	Non Line of Sight
NTIC	Nouvelles Technologies de l'Information et de la Communication
NB	Narrow Band
SNTD	Nombre des Slots Nécessaires pour la Transmission d'une trame de Données
OQ-PSK	Offset Quadrature PSK
PA	Points d'Accès
PAN	Personal Area Network
PDA	Personal Digital Assistant
PSSS	Parallel Sequence Spread Spectrum
QoS	Quality of Service
RAP	Random Access Phase
RFD	Reduce Function Device
RFID	Radio Frequency Identification Device
SB	Seuil Bas
SD	Superframe Duration
SH	Seuil Haut
SIFS	Short InterFrame Space

SIG	S pecial I nterest G roup
SMP	S ecurity M anagement P lan
SO	S uperframe O rders
TDMA	T ime D ivision M ultiple A ccess
TG6	T ask G roup 6
TIC	T echnologies de l' I nformation et de la C ommunication
TMB	T rafic M oyen B as
TMH	T rafic M oyen H aut
TOR	T out O u R ien
TU	T aux d' U tilisation
3GPP	T hird G eneration P artnership P roject
UUID	U niversally U nique I D
UWB	U ltrat W ide B and
VHP	V ery H igh P riority
WBAN	W ireless B ody A rea N etwork
WLAN	W ireless L ocal A rea N etworks
WPAN	W ireless P ersonal A rea N etworks
WSN	W ireless S ensor N etworks
WiFi	W ireless F idelity

Introduction générale

Contexte et motivation

Au cours des dernières années, les réseaux de capteurs ont vu leurs champs d'applications s'élargir pour toucher plusieurs domaines, dont (i) ceux de la surveillance des incendies, des fuites de gaz toxiques... (ii) des mesures et des collectes d'informations environnementales [1], de température, de divers indicateurs atmosphériques... (iii) et des applications militaires [2, 3].

Les domaines à vocation médicale et d'assistance aux personnes n'ont pas manqué de s'intéresser eux aussi à cette technologie émergente, face aux nombreux attraits qu'elle représente. En effet, vu leur taille réduite et leur faible coût, les nœuds capteurs peuvent s'insérer facilement et discrètement dans l'environnement d'un malade ou de toute personne nécessitant une surveillance continue, en particulier pour les personnes âgées ou handicapées [4] [5].

Pour ce public, utiliser un réseau de capteurs capable de collecter diverses mesures sur l'état de santé de la personne, ou surveillant tout changement suspect dans son environnement représente une solution très avantageuse pour plusieurs raisons. Sur le plan économique, surveiller une personne âgée tout en la gardant dans son environnement de vie habituel permettrait de diminuer les charges d'assistance aux personnes en les traitant par un personnel spécialisé à l'hôpital ou à une maison de retraite. Un apport non négligeable est lié au côté psychique et social de la personne âgée à qui cette surveillance discrète et imperceptible lui assurerait à la fois le sentiment de sécurité, de respect de la vie privée et d'autonomie.

L'utilisation de cette technologie a fait émerger des méthodes de travail et de réflexion transversales originales pour les chercheurs et industriels afin de résoudre les nouvelles problématiques qui touchent les disciplines liées aux problèmes économiques et de la santé dans l'objectif de proposer de nouvelles solutions technologiques qui associent des compétences transversales complémentaires pour résoudre des problèmes multidisciplinaires.

Une nouvelle discipline est apparue, représentant un point de rencontre entre les nouvelles technologies de l'information et de la communication et la santé publique, que l'on nomme *e-santé* [6].

L'*e-santé* vise, en particulier, à résoudre les problématiques liées au vieillissement de la population mondiale qui a mis en évidence des problèmes de santé et de dépendance des personnes âgées. Afin d'améliorer la condition de vie des aînés, des solutions sont proposées et se basent sur l'intégration des nouvelles technologies dans le système de santé. Ce nouveau domaine de recherche accorde un privilège à ses utilisateurs en rendant la vie plus simple et plus commode. L'impact de ses applications sur la vie de l'être humain est apprécié et demandé par la société car un grand nombre de tous ces besoins peuvent être satisfait par les applications de l'*e-santé*.

Plusieurs systèmes sont proposés comme le projet *CANet* [7, 8], celui de *raquette intelligente* [9, 10], mais aussi le projet *Co-Robo Cane* [11] qui utilisent des capteurs pour détecter des informations à partir de l'environnement ou du corps humain, puis qui traitent ces données localement ou à distance à travers des applications dédiées afin de fournir des indicateurs sur l'état de santé et le niveau de l'effort effectué par les personnes surveillées.

Ces applications introduisent de nouvelles méthodes pour effectuer les analyses et le suivi nécessaire à distance sans être obligé de se déplacer. Elles offrent des méthodes d'échange de données sûres qui facilitent les partages de contenus numériques entre un centre de traitement local ou distant et les capteurs qui collectent l'information de leur environnement naturel. Plusieurs projets sont proposés dans ce domaine, parmi eux, nous trouvons le projet *CANet* qui vise à surveiller une personne via des capteurs qui instrumentent une canne de marche communicante.

L'idée principale du projet *CANet* a germé suite à la constatation qu'il était intéressant de se baser sur l'instrumentation d'une canne de marche pour assurer le suivi non intrusif d'une personne âgée et aider ainsi son maintien à domicile. La canne est très largement utilisée pour se déplacer, se reposer, indiquer une direction ou une personne, et voir même se défendre. Nos aînés ont confiance en elle et la considèrent souvent comme un *compagnon de vie* à part entière. Cette constatation, confortée par une expérience familiale personnelle du Pr. Thierry Val, a nourri l'idée qui consiste à utiliser la canne comme un outil de surveillance, de suivi et de contrôle. Ceci est faisable avec l'avancement technologique actuel et l'acceptation par les personnes bénéficiaires de cette surveillance.

Le projet *CANet* regroupe plusieurs disciplines et compétences (informatique, électronique, médical...) qui coopèrent entre elles afin de transformer une simple canne en un système embarqué qui permet la surveillance non intrusive tout en respectant la vie privée des personnes âgées en les maintenant non tributaires de tout besoin d'aide supplémentaire, grâce à un système de communication entre la canne et un centre de surveillance, local dans le cas d'une maison de retraite, ou distant dans le cas d'un maintien à domicile.

Problématique

Une personne peut évoluer dans un environnement restreint en étant à domicile, comme elle peut se déplacer dans un environnement ouvert à l'extérieur. Le réseau de capteurs surveillant la personne doit être capable de la localiser à tout moment. Il doit aussi assurer l'acheminement adéquat des données collectées vers le centre de contrôle. Il est nécessaire, de ce fait, de proposer des architectures adaptatives pouvant détecter les changements environnementaux de la personne et adapter ainsi les moyens de communication et de localisation nécessaires pour assurer une connectivité continue avec le centre de contrôle.

Dans ce contexte, nous supposons que l'environnement d'une personne à surveiller sera muni de plusieurs capteurs assurant la collecte d'informations diverses sur la localisation et l'état de la personne. Les capteurs sont idéalement embarqués dans la canne utilisée par la personne âgée.

Le nombre de capteurs utilisés pour la collecte d'information nécessaire pour le suivi et le contrôle de l'état de santé de l'utilisateur de la canne dépend des pathologies et des signes définis pour chaque type de maladie. Pour cette raison, le type et le nombre de capteurs utilisés varient d'une canne à une autre. Aussi, sur la même canne, existe une multitude de capteurs qui n'ont pas obligatoirement les mêmes caractéristiques. Ces capteurs peuvent générer des données avec des caractéristiques et des exigences différentes, en particulier des données qui doivent être transmises dès leur réception, comme les données d'alerte ou les informations sur l'état de la santé de l'utilisateur.

Les informations générées vont passer, dans notre proposition d'architecture réseau, à travers la même couche physique et couche MAC vers un point d'accès fixe ou distant. Ceci pose un problème de respect des exigences de qualité de service, pour certains types de données, en particulier pour le trafic temps réel.

Nous avons donc besoin d'un mécanisme protocolaire qui permet la gestion de divers trafics émanant des différents capteurs de la canne afin de les transmettre sur l'interface radio de communication de cette dernière. Ce protocole prend en considération la diversité des sources d'information ou problème d'accord. Notre proposition doit limiter au maximum les modifications au niveau de la technologie d'accès au médium utilisée.

Nous allons donc proposer une architecture de communication, permettant la surveillance continue de personnes âgées évoluant dans leur environnement naturel, qui offre une infrastructure réseau fiable, pour divers services de surveillance, de mesures et d'acheminement de données vers un centre de contrôle éloigné (cabinet médical, membres de la famille, etc.). Cette architecture prévoit des moyens de communication permettant l'acheminement de données collectées vers le centre de contrôle. Les capteurs doivent être alors capables d'utiliser d'autres réseaux de communication pour atteindre cet objectif. Une utilisation des différentes technologies de communication sera envisagée.

Contribution de la thèse

Dans les sections précédentes, nous avons évoqué globalement les grands verrous à résoudre dans notre thèse. Notre premier axe de travail a concerné l'architecture et les technologies qui sont recommandées pour le projet *CANet*. La topologie globale du réseau proposé contient plusieurs niveaux, ce qui lui permet de s'adapter au besoin du projet. Les technologies que nous avons proposées sont différentes d'un niveau à un autre, ce qui permet de profiter pleinement des avantages de chacune d'elles. La technologie de transmission basée sur le standard IEEE 802.15.4 sera l'une d'entre elles, et un focus particulier nous amènera à contribuer à son adaptation pour le cahier des charges du projet *CANet*.

Après cette étude, nous nous sommes intéressés aux capteurs utilisés dans la canne. Le nombre de capteurs qui peuvent être embarqués dans la canne varie d'une situation médicale à une autre. Cette variation rend le traitement des données générées par la couche MAC difficile car chaque capteur a des caractéristiques qui ne sont pas obligatoirement identiques aux autres capteurs de la canne. Afin de résoudre cette problématique, nous avons effectué une étude sur les caractéristiques (débit, priorité, etc.) des capteurs de la canne. Dans cette étude, nous avons pu classer les capteurs en divers profils, ce qui nous a ramené à traiter des profils qui ont des caractéristiques semblables et généralisables.

Ces profils peuvent être composés en trois classes :

- profils des messages tolérants au délai,
- profils des messages à contrainte temporelle,
- profil des messages urgents.

Chaque classe a besoin d'une méthode de traitement et d'accès au médium différente. Afin de satisfaire chaque type de profil, nous avons proposé l'utilisation d'une couche de différenciation, qui représente notre deuxième contribution majeure. Cette couche de différenciation dispose des méthodes nécessaires pour reconnaître les profils et le traitement qui doit être réalisé pour chaque message envoyé par les couches applicatives différentes liées aux capteurs. Elle permet la classification des messages reçus en trois catégories selon la période de transmission utilisée pour chaque type de profils. Cette couche permet la détection de la présence d'état critique et d'état urgence.

Afin de donner la possibilité de transmettre des trames dans la période **CAP** (*Contention Access Period*) et **CFP** (*Contention Free Period*) par chaque nœud, nous avons proposé un algorithme qui se base sur l'utilisation de la primitive *purge* proposée par la norme IEEE 802.15.4. Notre proposition offre la possibilité d'utiliser les deux périodes **CAP** et **CFP** sans avoir des pertes de trame, grâce à l'utilisation de la *purge*, et permet de synchroniser l'envoi des trames dans les périodes adéquates à chaque type.

Pour avoir de bonnes performances sur notre réseau, et afin de compléter le travail sur la couche différenciation, nous avons effectué une étude de l'impact des paramètres [BO](#) et [SO](#) de la couche MAC de 802.15.4. La présence des différentes valeurs de [BO](#) et [SO](#) et la variation des types de trafic, nous ont permis de proposer une nouvelle méthode de gestion du trafic basée sur la sélection adaptée des valeurs de [BO](#) et [SO](#). Dans cette méthode, la couche MAC du coordinateur fait varier la valeur de [BO](#) et [SO](#) selon l'importance du trafic qui va être transmis dans le réseau. Nous avons proposé un algorithme qui permet le calcul de la valeur la plus adaptée au trafic généré par le nœud qui est dans un état critique.

Finalement, nous avons proposé une solution qui permet la transmission de la voix à travers la pile protocolaire de 802.15.4, en utilisant les résultats des travaux effectués sur la variation des valeurs de [BO](#) et [SO](#).

Structure du rapport

Dans cette section, après avoir présenté les problématiques et nos contributions, nous présentons le plan de notre thèse.

Le rapport de thèse est divisé en trois chapitres qui présentent notre étude théorique et nos contributions.

Dans le chapitre [1](#), nous présenterons brièvement le contexte dans lequel l'*e-santé* est apparu. Nous présenterons plusieurs projet qui ont été développés dans ce cadre, en particulier le projet *CANet*. Ensuite, nous introduirons les technologies qui pourront être utilisées dans ce projet. À la fin de cette section, nous décrivons les technologies les plus adéquates pour notre sujet de thèse.

La suite de ce manuscrit traitera de nos contributions : dans le chapitre [2](#), nous détaillerons nos travaux sur l'architecture de réseau et la transmission de données à travers la norme [IEEE](#) 802.15.4. Nous présenterons nos contributions dans ce domaine.

Le chapitre [3](#) détaillera nos résultats de simulation, suite à la modélisation de nos protocoles.

Finalement, nous conclurons à partir des résultats de nos travaux et discuterons des perspectives ultérieures de travail.

Chapitre 1

Systèmes d'aide aux personnes âgées et réseaux de communications adaptés

Les applications de l'*e-santé* sont le résultat d'une collaboration entre les domaines des technologies de l'information et de la communication (**TIC**), des systèmes électroniques embarqués, des capteurs et de la santé publique. Dans ce premier chapitre, nous commencerons par présenter d'une manière générale le domaine *e-santé* et les principales applications existantes. Ensuite, nous présenterons différents types de réseaux de communications associés, en précisant les détails nécessaires pour comprendre le cheminement dans nos contributions de la thèse.

1.1 E-santé et applications

1.1.1 L'e-santé

Le monde actuel connaît de profondes mutations démographiques qui ont conduit à l'apparition du phénomène du vieillissement de la population et de la longévité [12].

Le nombre des personnes qui ont 65 ans ou plus dans le monde était égal à 760 millions en 2010, il devrait atteindre 1 milliard à la fin de 2020 [13] et 2 milliards en 2050 [12]. Les projections pour 2150 montrent que le nombre de personnes âgées devrait atteindre un tiers de la population mondiale ce qui rend l'objectif de vieillir en bonne santé un point prioritaire au niveau européen [14].

Par exemple, la France a initié la préparation d'une loi qui vise l'adaptation de la société au vieillissement [15] et qui se décline en trois volets : prévention de la perte d'autonomie, adaptation de la société et accompagnement et maintien à domicile.

Aussi, au niveau européen, la stratégie du “**bien vieillir**” a été mise en place. Cette stratégie met l'accent sur trois points importants [14] : la prévention, le dépistage et le diagnostic précoce, les soins et les traitements et l'activité et l'autonomie des personnes âgées. Cette initiative a ouvert une nouvelle porte à la recherche et au développement. L'objectif des recherches actuelles est de proposer une solution qui permette de garder l'indépendance de la personne âgée tout en utilisant les dernières innovations dans les domaines de la santé et des nouvelles technologies de l'information et de la communication (NTIC) pour assurer le bon traitement moral, physique et médical. Cet objectif est offert par les applications *e-santé*, en particulier celles qui permettent le contrôle et le suivi à domicile sans l'intervention d'autres personnes sauf dans le cas d'urgence ou à la demande des personnes âgées.

La notion de *e-santé*, désignée également par *e-health*, télésanté ou cyber santé, est utilisée pour la première fois en 1999 par John Mitchell [16]. La définition la plus connue et la plus utilisée est celle proposée par Eysenbach [6] : “*E-health est un domaine émergent créé par l'intersection entre les domaines de l'informatique médicale, la santé publique et le secteur privé. Ce domaine fait référence au service de santé et les informations en matière de santé à travers Internet ou d'autres technologies connexes...*”

L'intégration des nouvelles technologies dans le domaine de la santé publique est la clé qui a permis d'ouvrir une nouvelle époque d'évolution au niveau matériel afin de fournir une multitude d'informations qui n'étaient pas disponibles par le passé. Cette évolution est à l'origine de l'amélioration de la qualité des données fournies aux équipes médicales pour les aider à prendre des décisions qui seront de plus en plus précises et concrètes dans le futur. L'émergence des technologies médicales, telles que les technologies de suivi et de contrôle, dans le monde entier, a permis à de nouvelles applications d'être installées et utilisées dans de nombreux environnements. L'exploitation de cette technologie dans les domiciles et les résidences représente une bonne solution pour le bien-être des personnes âgées puisque les garder dans le même environnement assure la stabilité psychologique et en même temps un suivi meilleur tout en gardant les services offerts par les centres médicaux et les hôpitaux. La détection des situations anormales se fait d'une manière instantanée et l'intervention humaine s'effectue seulement en cas de besoin. Différentes applications sont proposées dans ce cadre et peuvent être réparties en trois classes [17]:

- soins à domicile,
- soins à la résidence spécialisée,
- soins intensifs.

Afin d'assurer l'équilibre entre la qualité de vie et le coût des soins, un compromis entre les deux doit être trouvé. Pour augmenter la qualité de vie, il faut conserver les conditions d'une vie ordinaire (chez soi) et effectuer le contrôle d'une manière non intrusive sans que cela ne soit trop coûteux. Cependant, pour augmenter la qualité des soins, il faut disposer d'une équipe médicale spécialiste qui veille sur la santé de la personne âgée, ce qui est onéreux.

L'amélioration du concept de soin est passé par plusieurs étapes où les inventions technologiques représentent un catalyseur très important (Smartphone, capteurs...) permettant la détection et le transfert d'information. Il devient alors nécessaire de mettre en évidence le problème de la différenciation des services relatifs à ces informations.

Le nombre de **WPAN** (*Wireless Personal Area Networks*) et **WLAN** (*Wireless Local Area Networks*) utilisés dans les hôpitaux, maisons de retraite ou à domicile est en constante augmentation. La qualité et l'importance des données collectées demandent un certain niveau d'assurance en terme de fiabilité du réseau : l'information doit arriver au récepteur ou au point de collecte d'information de façon certaine, avec une latence maîtrisée et en temps réel avec différents niveaux de priorité.

Les services *e-santé* doivent être totalement fiables et efficaces. Les technologies utilisées dans l'*e-santé* doivent soutenir différents niveaux de qualité de services (**QoS**). Plusieurs travaux de recherche académiques et industriels ont été initiés afin de créer une nouvelle solution technologique qui puisse satisfaire les exigences des applications *e-santé* en matière de bande passante, fiabilité et faible latence.

1.1.2 Quelques applications de l'e-santé

Dans cette section, nous présentons quelques projets *e-santé* basés sur l'utilisation des **WSN** (*Wireless Sensor Networks*) pour le suivi de personnes. Nous présenterons des exemples de projets destinés aux personnes dépendantes et d'autres utilisés dans le domaine sportif.

1.1.2.1 Co-robo Cane : le robot qui vit dans la canne

Le projet Co-Robo cane a été imaginé essentiellement pour aider les personnes aveugles ou mal voyantes en utilisant la canne comme un élément d'orientation et de reconnaissance de l'environnement [18]. La canne collabore avec l'utilisateur à travers une interface homme-machine vocale afin de l'accompagner en le conduisant jusqu'à sa destination.

Le système embarqué dans la canne doit être capable de détecter les obstacles (portes, murs, escaliers...) et apte à reconnaître les objets. Afin d'accomplir les services demandés, la canne est équipée d'une multitude de capteurs (une caméra, un détecteur laser, etc.) qui permettent de connaître l'environnement, la position et de détecter les obstacles dans la trajectoire de l'utilisateur.

Ce projet était initié par l'université de l'Arkansas en 2013 et subventionné par *National Institute of Biomedical Imaging and Bioengineering* et *National Eye Institute of the National Institutes of Health*. Un prototype a été réalisé en 2014. Il était utilisé, essentiellement, pour la collecte de données pour effectuer une étude préliminaire.

1.1.2.2 THE AID : Une canne de gestion de santé personnelle

Ce projet vise la réintégration des personnes âgées dans la société en les aidant dans leurs activités quotidiennes.

Le projet THE AID propose d'équiper une canne de marche avec une multitude de capteurs qui permet de mesurer le pouls, la tension et la température corporelle de l'utilisateur lorsque l'avant-bras est en contact avec la canne. Les informations détectées sont affichées sur un afficheur **LCD** (*Liquid Crystal Display*). De plus, la canne doit être équipée d'un système de géo-localisation et de communication, ce qui permet à l'utilisateur de réaliser un appel d'urgence pour avoir une assistance et pour l'aider à trouver son chemin en transmettant l'information en communication directe par l'intermédiaire d'une oreillette [19].

1.1.2.3 Canne intelligente : Le successeur réaliste de THE AID

Le projet Canne intelligente, initié par Fujitsu, représente une amélioration du projet THE AID puisque l'objectif est ici de guider la personne âgée quand elle quitte son domicile et ainsi sans avoir de craintes de se perdre [19] et de rassurer ses proches par la transmission de sa position grâce à un logiciel spécifique qui permet de suivre les déplacements de la canne [20]. Le projet Canne intelligente se base sur un **GPS** (*Global Positioning System*), une liaison **WPAN** Bluetooth, un **WLAN Wifi** (*Wireless Fidelity*), des capteurs biométriques permettant la surveillance de l'état de santé de l'utilisateur.

L'utilisateur de la canne enregistre un itinéraire à l'avance par l'utilisation d'un logiciel spécifique. L'écran joue ensuite le rôle de guide grâce à l'affichage de flèches de directions et des vibrations au niveau de la poignée de la main de l'utilisateur lorsqu'il doit prendre une autre direction. De plus, l'afficheur a la capacité d'afficher les signes de fatigue et de montrer à la personne âgée le chemin qui lui permet d'arriver au lieu le plus proche où elle pourra se reposer [20]. La canne intègre aussi un capteur de rythme cardiaque qui s'active lorsque l'utilisateur pose sa main sur la poignée.

Un prototype a été dévoilé par Fujitsu au *Mobile World Congress* 2013. Malheureusement, ce prototype présente un défaut de taille : son autonomie n'est que de trois heures. Ceci est très insuffisant pour une utilisation continue sur toute une journée.

1.1.2.4 Le projet CANet

L'idée du projet *CANet* [7, 8] est née au sein de l'équipe de recherche SCSF du laboratoire LATTIS de l'Université de Toulouse 2, il y a maintenant 4 ans. *CANet* a pour but d'offrir la surveillance et le suivi d'une personne âgée sans être intrusif, c'est-à-dire sans équiper si possible directement la personne. Pour cette raison, les concepteurs ont cherché à identifier l'élément le plus habituel pour les personnes âgées. En se basant sur des expériences familiales personnelles, ils se sont aperçus que la canne est l'objet

le plus utilisé et le plus important pour la personne âgée. Ils ont décidé d'intégrer une multitude de capteurs biométriques qui permet la détection des informations liées à l'environnement et des informations sur l'état de santé de la personne âgée. Parmi ces capteurs, nous trouvons des capteurs de température de la main et de l'extérieur, un capteur d'humidité, un capteur de rythme cardiaque, un capteur de pression, un système de localisation, un système de communication sans fil... La canne contient également un microphone et un haut-parleur, ce qui permet la communication avec un centre de traitement ou un proche de la personne âgée. Ce projet a permis la fédération de différentes compétences auprès des chercheurs de l'IUT de Blagnac : informatique, électronique, réseaux, protocoles, mécanique, psychologie, expression et communications... Nous détaillerons dans le chapitre 2 le volet réseaux et protocoles de ce projet qui nous concerne plus particulièrement.

1.1.2.5 FWD Powershot

L'utilisation de la technologie s'est également généralisée dans plusieurs sports, collectifs et individuels. Parmi ces sports, nous citons le Hockey. Il représente un sport d'équipe, il se joue sur une patinoire spécialement aménagée, où les joueurs utilisent un bâton incurvé (appelé bâton de Hockey, *cross* en France ou canne de hockey en Belgique) pour frapper un disque en plastique (appelé rondelle ou palet) afin de marquer des buts dans les cages de l'adversaire. Les performances des joueurs dans ce jeu est très importante, donc connaître finement leurs performances sera un élément crucial. L'accès à ce type d'informations est devenu possible, de nos jours, avec le développement technologique. Dans ce cadre, une solution technologique offerte par le projet *FWD Powershot* propose d'équiper le bâton de *Hockey* par une multitude de capteurs qui permet de mesurer l'accélération et la vitesse de frappe de rondelle, la durée et l'angle des mouvements effectués par le joueur et sa vitesse de rotation. Le système transmet ensuite les informations collectées par l'intermédiaire d'un lien Bluetooth à un terminal de type Smartphone pour effectuer les traitements nécessaires et visualiser les résultats. Cette application permet de connaître les performances des joueurs dans une situation réelle et de les comparer par rapport aux mesures effectuées dans l'entraînement ou dans les matchs précédents [21, 22].

1.1.2.6 Intelligent Racquet

Le projet *Intelligent Racquet* était initié par la société française Babolat et développé en collaboration avec la société Movea. Les développeurs des deux sociétés proposent d'équiper la raquette par un accéléromètre, un gyroscope et un microprocesseur pour la transmission et la collecte des données. À partir des données collectées par les capteurs, l'application peut fournir des informations sur la puissance de frappe, zone d'impact de la balle, type, nombre de coups (coup droit, revers, service, smash) et les compétences techniques d'un joueur de tennis... Les méthodes utilisées pour traiter les informations collectées ne sont pas dévoilées par les sociétés.

Toutes ces informations collectées par les capteurs peuvent être transmises vers un *Smartphone* ou une tablette via Bluetooth afin d'être analysées. Ce système permet de constituer une base de données des informations qui aide à suivre l'amélioration technique et physique du tennisman [9, 23].

1.1.2.7 Discussion

Dans cette section nous avons présenté des applications *e-santé* qui touchent plusieurs domaines. La plupart des applications proposent un traitement local des données qui seront affichées sur l'interface d'un Smartphone ou une tablette.

La solution *Co-robot cane* est dédiée aux personnes mal voyantes ou aveugles. Le projet propose une solution pour les guider. Les données collectées seront traitées localement et communiquées à l'utilisateur à travers une interface homme-machine.

Les projets *intelligents racquet* et *FWD Powershot* sont des solutions pour les sportifs (amateurs ou professionnels). Ils permettent le traitement d'une multitude de données collectées par les capteurs afin de fournir des informations sur les performances et l'évolution technique du joueur.

Le projet *The AID* n'a pas abouti sur la réalisation d'un prototype, mais était une base utilisée par Fujitsu pour créer l'idée d'une *cane intelligente* qui peut guider l'utilisateur à travers un itinéraire fixé d'avance. Les directions sont indiquées à travers l'affichage des flèches sur une interface LCD et dans l'oreillette. Ce projet se différencie par rapport au projet *Co-robot cane* par la transmission de la position de la cane et des informations sur le rythme cardiaque de l'utilisateur à travers un logiciel spécifique.

Le projet *CANet* représente une évolution significative au niveau des fonctionnalités offertes. Ce projet propose d'intégrer une multitude de capteurs qui permet de suivre l'état de santé des personnes âgées. Contrairement aux autres projets, il propose de transmettre les données vitales en temps réel. Ces données seront traitées par des systèmes spécifiques. De plus, il offre la possibilité d'établir une communication vocale avec l'utilisateur, ce qui lui permet d'être rassuré et en confiance. Le projet *CANet* peut être vu comme un système de contrôle, de suivi et de communication. Le rassemblement de toutes ces propriétés et le fait d'être non intrusif le rendent très évolutif par rapport aux projets proposés pour la même tranche d'âge qui est très sensible.

Les besoins des applications de ce nouveau domaine, en particulier pour le projet *CANet*, exigent certains critères qui doivent être assurés par les technologies utilisées. Dans le monde industriel et universitaire, quatre technologies sont connues par leurs performances et leurs faibles consommations d'énergie : **ANT** (*Advanced and adaptive Network Technology*) [24], **IEEE** (*Institute of Electrical and Electronics Engineers*) 802.15.4 [20] (avec ses versions de 2006 et 2011), **IEEE** 802.15.6-2012 [25] et **BLE** (*Bluetooth Low Energy*) [26]. Ces quatre technologies se présentent comme des candidates pour régner sur les **PAN** (*Personal Area Network*) et **BAN** (*Body Area Network*).

Dans la partie suivante, nous présentons ces différentes technologies en détail, ce qui nous permettra ensuite de choisir celle qui est la plus adaptée aux besoins du projet *CANet*.

1.2 Technologies des réseaux sans fil

L'intégration des technologies radiofréquences et ses dérivées sans fil dans le cycle de la vie humaine a ouvert la possibilité d'avoir une multitude de choix qui prennent en compte les différentes spécifications et exigences humaines, du point de vue de l'acceptation, des habitudes et des applicatifs. L'*e-santé* est considéré parmi les domaines les plus exigeants, une multitude de normes et des technologies sont désignées comme par exemple : les normes [IEEE 802.15.4](#), [IEEE 802.15.6](#), [ANT](#) ou des versions spécifiquement adaptées de [Wifi](#) et [BLE](#) pour répondre aux besoins des applications *e-santé*.

1.2.1 Analyse des architectures réseaux adaptées

Plusieurs architectures sont proposées pour les réseaux filaires. Mais, elles ne sont pas toutes applicables sur les réseaux sans fil. Pour cette raison, généralement, seulement trois modèles topologiques sont considérés : la topologie maillée, la topologie en arbre et l'étoile.

L'étoile représente un réseau qui peut être soit point à point dans le cas de l'existence de deux nœuds seulement, soit point à multipoint ou multipoint à point, s'il existe un plus grand nombre de nœuds. Cette topologie contient un nœud fixe qui joue le rôle du nœud central, par exemple un point d'accès ou un serveur, et des nœuds terminaux qui sont en communication avec ce dernier uniquement.

Dans la topologie en arbre, nommée aussi la topologie hiérarchique, la connexion entre les nœuds se fait d'une manière progressive et donc hiérarchique. Au sommet de l'arbre, nous trouvons le nœud racine qui est connecté à des nœuds fils, et ceci de façon récursive.

Dans les deux topologies arbre et étoile, une connexion défectueuse n'affecte pas tout le réseau. Cependant, si le nœud central et le nœud racine font défaut, les nœuds connectés ne peuvent plus communiquer. La simplicité et la faible consommation d'énergie des nœuds, sauf pour le nœud central et racine représentent les plus importants avantages de ces deux architectures. Pour le cas de l'étoile, on constate également une latence faible de communication entre les nœuds, ce qui n'est pas vrai pour un arbre dont la profondeur est importante.

La topologie maillée représente souvent une évolution de l'architecture étoile. Dans cette architecture, un nœud peut avoir plusieurs liaisons point à point. L'inconvénient de cette topologie est situé dans le grand nombre de connexions qui peuvent être établies par un nœud, ce qui influence énormément ses performances et augmente considérablement la consommation de l'énergie. Aussi, le passage des messages envoyés par les émetteurs via

plusieurs intermédiaires avant d'arriver à leur destination induit une latence importante. Mais cette topologie offre une possibilité de passage à grande échelle avec redondance et tolérance aux fautes acceptables.

Afin de profiter des avantages de chaque topologie présentées ci-dessus, des topologies hybrides entre celles de l'étoile, de l'arbre et de la maillée (ou *MESH*) ont été proposées, comme les arbres d'étoiles... Ces topologies offrent des communications robustes et la possibilité de minimiser la consommation d'énergie pour les noeuds autonomes. Les topologies linéaires et en anneau restent cantonnées à des applicatifs particuliers liés à des espaces géographiques spécifiques.

1.2.2 Différentes technologies potentielles

L'utilisation effective par le grand-public des réseaux sans fil a commencé par l'adoption de la norme [IEEE 802.11](#) en 2007. Plusieurs versions de la norme [IEEE 802.11](#) sont apparues conformément aux exigences et aux besoins de ces nouvelles applications. Mais la miniaturisation des composants électroniques et l'utilisation de la technologie dans des contextes réels avec des capteurs ont permis d'identifier certaines faiblesses de la norme. Les problèmes notables détectés, vitaux pour certaines applications, sont l'autonomie énergétique et le passage à l'échelle.

La proposition de nouvelles solutions par la communauté scientifique et les industriels a permis d'avoir une multitude de technologies comme [IEEE 802.15.4](#), [ANT](#), *WirelessHART* [27]... La mise en place de ces technologies dépend de la vision de son concepteur; pour cette raison, certaines de ces technologies ont proposé des améliorations techniques et des méthodes initiées par [IEEE 802.11](#), d'autres ont proposé des nouvelles technologies basées sur des concepts novateurs.

Dans cette partie, nous présentons les principales technologies qui sont potentiellement les plus adaptées à notre besoin [IEEE 802.15.4](#) (2006 et 2011), [ANT](#), [IEEE 802.15.6-2012](#) et [BLE](#).

1.2.2.1 De Bluetooth à BLE

1.2.2.1.1 Apparition de BLE

La technologie Bluetooth a été mise au point en 1994, initialement par Ericsson [26]. En 1998, un groupe d'industriels a formé le groupe Bluetooth SIG (*Special Interest Group*) afin de produire la première spécification (*Bluetooth 1*) publiée en 1999 [28].

Bluetooth a été standardisé sous la norme IEEE 802.15.1 en 2002. Le groupe SIG a pris en charge la continuité de cette technologie par l'élaboration d'un cahier des charges, géré le programme de qualification et la protection de la marque.

Cette technologie est passée par différentes étapes d'amélioration à partir de la version V1.0 jusqu'à la version V3.0+HS (*Headset*), sujette alors à des tentatives pour intégrer UWB (*Ultra Wide Band*). Ce transfert de technologie a été effectué par l'alliance *Wi-Media* en 2009. En 2010, la version 4.0 [29] ou BLE a été adoptée. Cette nouvelle version représente une amélioration radicale dans le parcours d'évolution de Bluetooth, elle permet l'utilisation de deux technologies différentes : *Bluetooth* classique BR/EDR (*Basic Rate/Enhanced Data Rate*) et BLE, qui peuvent fonctionner séparément ou se compléter. L'utilisation de la technologie à faible consommation permet à certains appareils équipés de piles boutons ou de petites batteries d'utiliser la technologie *Bluetooth*. Dans cette partie, nous allons nous intéresser, en particulier, à cette nouvelle technologie BLE intégrée dans *Bluetooth*.

La technologie BLE a hérité de la pile protocolaire du *Bluetooth* classique [30] qui peut être adaptée à deux types de noeuds : le contrôleur et l'hôte (cf. Figure 1.1). Mais, les deux piles protocolaires sont incompatibles, ce qui rend la communication directe entre un noeud BLE et un autre noeud d'une version de *Bluetooth* antérieure à V4.0 impossible.

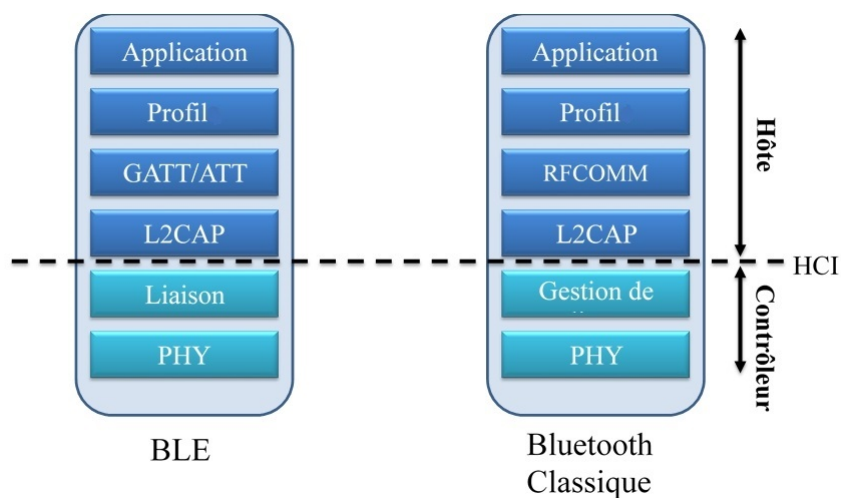


FIGURE 1.1: Comparaison entre les piles protocolaire de BLE et Bluetooth classique

Pour surmonter cette incompatibilité, la spécification de *Bluetooth* V4.0 a défini deux types de noeuds : *Single Mode* (**BLE**, *Bluetooth Smart*) et *Dual Mode* (**BR/EDR/BLE**, *Bluetooth Smart Ready*) [31].

Dans le *Single mode*, le nœud implémente la couche protocolaire de **BLE**. Donc, il peut communiquer avec les noeuds de type *Single Mode* ou *Dual Mode* [31] (cf. Figure 1.2). Les noeuds de type *Dual Mode* implémentent les piles protocolaires de *Bluetooth* classique (**BR/EDR**) et **BLE**, ce qui leur permet de communiquer avec n'importe quel nœud dans le réseau [31] (cf. Figure 1.2).

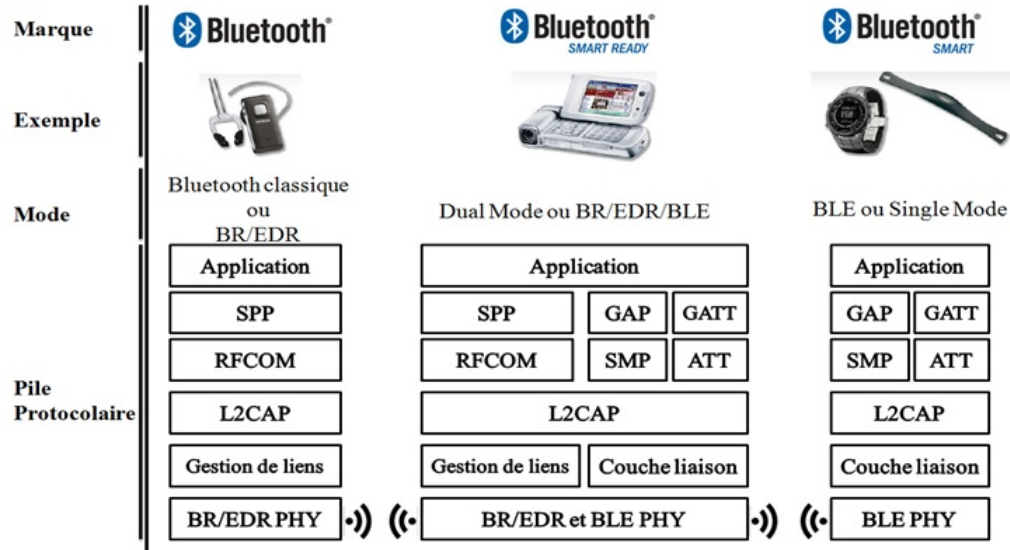


FIGURE 1.2: Relation entre les différentes versions de Bluetooth [31]

1.2.2.1.2 Couche physique et topologies de BLE

Comme les versions précédentes de *Bluetooth*, **BLE** fonctionne dans la bande **ISM** (*Industrial, Scientific and Medical*) 2.4 GHz et il définit 40 canaux avec un espace entre deux fréquences centrales égales à 2 MHz [32]. Parmi les canaux définis, la couche liaison utilise les 3 canaux 0, 12 et 39 appelés *advertising channels* pour la détection de présence des nœuds distants, l'établissement de communication et les transmissions en *Broadcast*. Ces canaux sont choisis dans la bande de fréquences où il n'existe pas de canaux définis par la technologie **Wifi** (précisément les canaux 1, 6 et 11) [32]. Les 37 canaux restants sont utilisés pour la transmission des données.

Afin de surmonter la problématique d'interférence avec les autres technologies qui utilisent la bande ISM, le **SIG** et l'**IEEE** [32] ont développé deux approches dans le but d'atténuer l'interférence entre *Bluetooth* v1.1 et **Wifi** initialement : une approche non collaborative comme **AFH** (*Adaptive Frequency Hopping*) et une approche collaborative comme **TDMA** (*Time Division Multiple Access*) [33]. **BLE** hérite de *Bluetooth* la technique **AFH** [34] (en réduisant le nombre de canaux utilisé de 32 à 3 canaux uniquement) et les problèmes inhérents aux transmissions sans fil comme le *fading*, et le multitrajet [32, 33]. Le débit de transmission dans **BLE** atteint alors théoriquement 1 Mbit/s.

La nouvelle version de *Bluetooth* a énormément simplifié la topologie puisqu'elle supporte uniquement une topologie étoile (appelée *Piconet*) composée d'un *Master* et un ou plusieurs *Slaves* (les deux rôles *Master* et *Slave* sont définis au niveau de la couche liaison). Un *Master* est chargé de gérer la communication avec le *Slave*. S'il existe plusieurs *Slaves* dans un même *Piconet*, le *Master* est alors chargé de la gestion de communication entre ces derniers. Un noeud *Master* peut gérer théoriquement 2^{31} *Slaves*.

Contrairement au *Bluetooth* classique, les noeuds *Slaves* peuvent établir une connexion avec un seul *Master*, ce qui signifie qu'un *Slave* ne peut être que dans un seul *Piconet*. Aussi, ils n'ont pas la possibilité de jouer le rôle d'un *Master* et *Slave* en même temps [35].

Dans un *Piconet*, nous pouvons avoir deux types de communications : unidirectionnelle et bidirectionnelle. Dans la communication unidirectionnelle, le noeud envoie les données en diffusion dans des trames d'annonce à travers l'*advertising channel* (l'émetteur est appelé *Advertiser* et le récepteur des trames appelé *Scanner*). Ce cas de communication peut être utilisé dans la transmission des messages générés périodiquement comme une transmission régulière de la température.

La communication bidirectionnelle demande un établissement de connexion entre les noeuds qui vont échanger des données. L'établissement de connexion est une procédure asymétrique où un noeud envoie une annonce à travers l'*advertising channel* pour informer les autres noeuds, appelés *Initiator*, qu'il est disponible. Si un *Initiator* entend un *Advertiser* et décide d'établir une connexion avec lui, il envoie une demande de connexion. Une connexion de type point à point est créée entre l'*Initiator* et l'*Advertiser*. Le *Master* et le *Slave* agissent comme un *Initiator* et *Advertiser* respectivement [32].

L'intérêt de **BLE** est la conservation de l'énergie qui est possible grâce à l'état de sommeil de la majorité des noeuds *Slave*. Les noeuds se réveillent périodiquement pour la réception des trames [32, 35] dans les instants de transmissions déterminés par *Master*.

La coordination de l'accès au médium s'effectue avec l'utilisation du **TDMA**. Les informations nécessaires pour le bon déroulement de la communication et la transmission des données sont envoyées dans la demande d'établissement de connexion [32, 35]. Ces informations peuvent être échangées tout au long de la connexion pour plusieurs raisons comme le changement de canal de données utilisé [32].

La connexion est considérée ouverte tant que l'échange des trames entre le *Master* et le *Slave* est en cours. Après la fermeture de connexion, le *Slave* entre dans l'état sommeil jusqu'au début du *connection event* suivant. La fréquence radio utilisée dans le nouveau *connection event* est calculée par l'algorithme **AFH**. Le temps entre deux connexions consécutives varie entre 7.5 ms et 4 s.

Le format de la trame utilisée dans **BLE** est simplifiée par rapport à *Bluetooth* V3.0. Elle supporte tous les types de transactions possibles.

Jusqu'à présent, nous avons présenté les éléments essentiels de la partie contrôleur qui définit la couche liaison et la couche physique de **BLE**. L'interface de contrôle (**HCI**) (cf. Figure 1.1) se positionne comme une interface intermédiaire entre l'hôte et le contrôleur. L'interface **HCI** de **BLE** n'est qu'une évolution de celle de *Bluetooth* classique avec une minimisation du nombre des commandes possibles pour la rendre adaptée aux exigences des applications ciblées (des applications pour les loisirs, le travail ...) par **BLE** [46]. Cette interface fournit un ensemble d'API au-dessus de la couche liaison afin de simplifier la tâche d'implémentation des services.

1.2.2.1.3 Pile protocolaire de BLE

Au-dessus de l'interface **HCI**, nous trouvons **L2CAP** (**L**ink **L**ayer **C**ommon **A**da**P**tation layer) qui utilise un protocole équivalent à celui de *Bluetooth* classique, mais simplifié et optimisé. Le but essentiel de **L2CAP** est de multiplexer les données de 3 protocoles utilisés dans les couches supérieures : **ATT** (**A**tttribute **P**rotocol), **SMP** (**S**ecurity **M**anagement **P**lan) et la signalisation de la couche liaison. Les données de ces trois protocoles sont transmises en rafale et sans mécanisme de retransmission et de contrôle de flux [9, 32].

BLE est conçu pour la transmission des états d'information par l'utilisation de l'**ATT** et **GATT** (**G**eneric **A**tttribute **P**rofile) qui représentent les piliers de cette nouvelle architecture. Les deux couches **ATT** et **GATT** représentent un changement énorme dans la philosophie avec l'existence de ces protocoles supplémentaires et les définitions de nouveaux formats de données qui sont utilisées par les couches supérieures. Elles définissent les attributs, les caractéristiques et les services assurant ainsi l'interopérabilité entre les différents appareils qui utilisent le *Bluetooth* classique ou **BLE**. L'**ATT** définit la communication entre deux noeuds qui jouent le rôle de client et serveur respectivement. Le serveur maintient un ensemble d'attributs qui sont des structures de données utilisées par **GATT**. Les rôles de clients et de serveurs sont définis au niveau du **GATT**, et sont donc indépendants du rôle de *master* ou *slave* défini par la couche liaison [32].

Le **GATT** définit un *framework* qui utilise l'**ATT** pour la découverte des services et l'échange des caractéristiques d'un noeud à un autre. Les caractéristiques sont des données qui contiennent une valeur et des propriétés. Ces données sont liées à des services et des caractéristiques qui sont stockées dans des attributs.

Au-dessous de **GATT** et **ATT**, nous trouvons le **GAP** (**G**eneric **A**ccess **P**rofile) qui spécifie le rôle du noeud, les modes et méthodes de découverte des autres noeuds et des services, la gestion de l'établissement de connexion et la gestion de la sécurité.

1.2.2.1.4 Rôles définis pour le BLE

La spécification de **BLE** introduit également un nouveau concept de profil appelé rôle qui décrit les fonctionnalités de base implémentées dans un noeud. Quatre rôles sont définis : *Broadcaster*, *Observer*, *Peripheral*, *Central*.

Si le noeud joue le rôle de *Broadcaster* (cf. Figure 1.3-a), il diffuse seulement des données à travers les canaux *Advertising*. Dans ce rôle, le noeud ne supporte pas l'établissement de connexion avec les autres noeuds. Le rôle *Observer* est relié directement au rôle *Broadcaster* puisqu'il est joué par le noeud récepteur dans le cas de diffusions d'informations. Ces rôles sont utilisés dans le cas d'une communication unidirectionnelle [28, 32].

Les noeuds responsables de l'initiation et la gestion de plusieurs connexions jouent le rôle *Central* (cf. Figure 1.3-b), alors que le rôle *Peripheral* est dédié aux noeuds qui communiquent avec le noeud *Central*. En conséquence, les deux rôles *Central* et *Peripheral* sont restreints à une communication bidirectionnelle [28, 32]. Un noeud tolère l'utilisation de plusieurs rôles, mais il ne joue qu'un seul rôle à la fois pour une durée donnée.

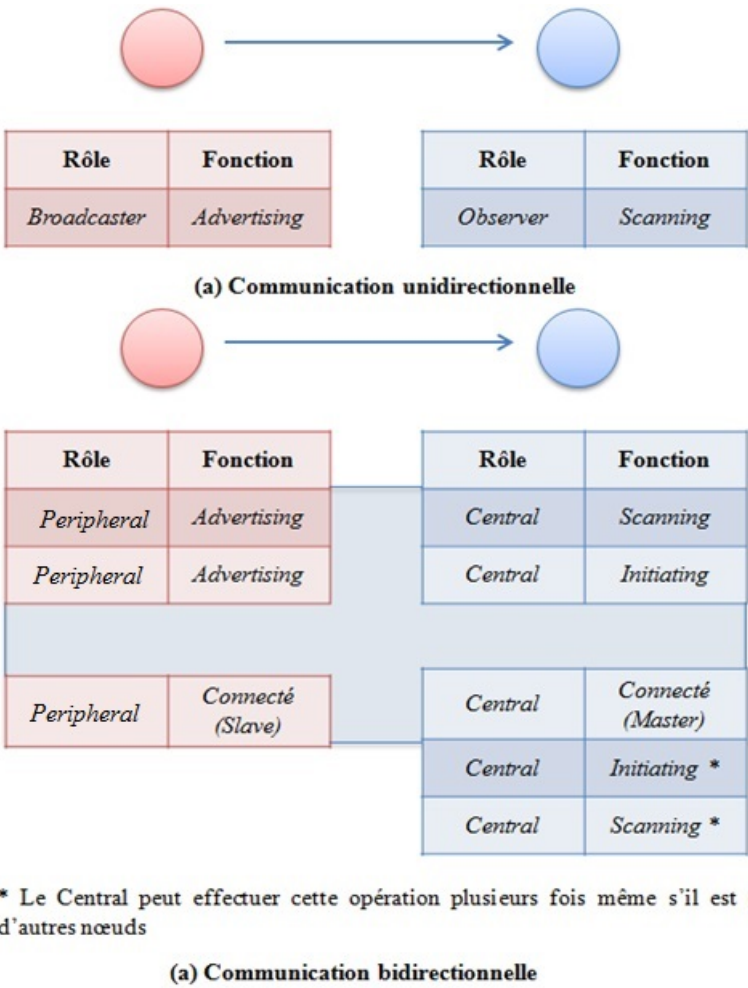


FIGURE 1.3: Différents rôles de BLE avec les fonctionnalités utilisées

Cette diversité de rôles définis dans le *GAP* permet l'amélioration de la gestion de l'énergie dans *BLE* où les noeuds passent la majorité du temps à l'état sommeil. Les états utilisés dans chaque type de noeuds, afin de réaliser le comportement demandé, sont présentés dans les Figure 1.4 et Figure 1.5. Le diagramme d'état d'un noeud qui joue

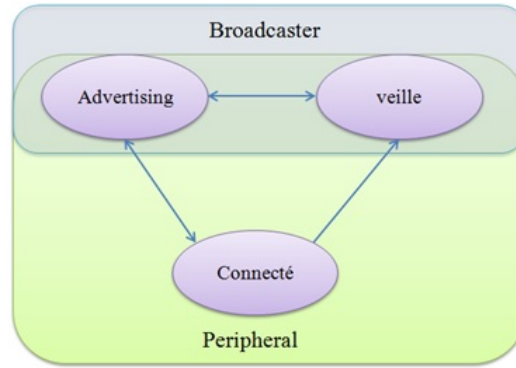


FIGURE 1.4: Diagramme d'état des noeuds BLE *Broadcaster* et *Peripheral* [32]

le rôle d'un *Broadcaster* ou *Peripheral* est composé de 3 états : *Advertising*, connecté et veille. Le noeud *Broadcaster* ne peut pas accéder à l'état connecté (Figure 1.4).

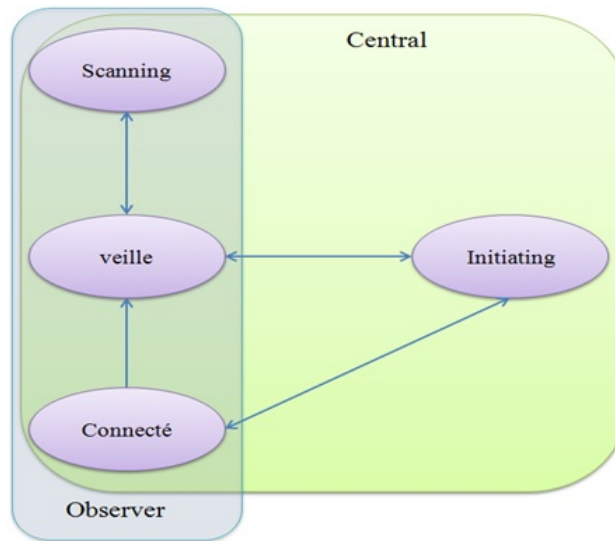


FIGURE 1.5: Diagramme d'état des noeuds BLE *Observer* et *Central* [32]

La Figure 1.5 présente l'ensemble des états d'un noeud *Observer* et *Central*. Un noeud qui joue le rôle d'un *Observer* ne peut pas accéder à l'état d'initialisation (*initiating*).

Dans la spécification v4.1 (sortie en 2013), toutes les contraintes sur les combinaisons entre les rôles sont supprimées, donc [31, 32] :

- un noeud peut jouer le rôle d'un *Central* et *Peripheral* en même temps,
- un *Central* peut être connecté à plusieurs *Peripherals*,
- un *Peripheral* peut être connecté à plusieurs *Centrals*.

Bluetooth V4.1 propose de nouvelles fonctionnalités pour suivre les nouvelles tendances au niveau des réseaux sans fil à faible consommation pour l'Internet des Objets et **IPV6** (*Internet Protocol Version 6*). Parmi les nouveautés, nous pouvons citer [31] :

- une évolution résolument tournée vers l'Internet des Objets,
- une interopérabilité accrue.

Cette technologie est passée par plusieurs étapes d'amélioration et d'adaptation aux besoins de l'utilisateur. Comme elle est utilisée par la majorité des appareils électroniques comme les *Smartphones*, les ordinateurs portables et les tablettes, elle représente un concurrent extrêmement fort pour les technologies à faible consommation existantes comme la norme IEEE 802.15.4. BLE aurait sans doute été un bon candidat pour être utilisé dans notre thèse mais est apparu que très récemment, bien après le début de nos travaux. Dans la partie suivante, nous allons présenter le standard IEEE 802.15.4 afin de mieux le connaître et repérer les points de différence avec BLE.

1.2.2.2 La norme IEEE 802.15.4-2006

Les technologies sans fil initiales, originellement Wifi et Bluetooth, prenaient peu en considération la consommation d'énergie, ce qui a limité leurs utilisations à des appareils non contraints énergétiquement ou des équipements autonomes qui ne sont capables que de disposer de l'énergie nécessaire pour quelques heures d'utilisation en continu. En 1998, les premiers signes d'une nouvelle technologie commencent à se faire sentir. Cette technologie ouvre aux industriels des champs d'applications qui n'étaient pas envisageables dans le cadre des anciennes technologies.

En 2003, le premier standard IEEE 802.15.4-2003 [36] est publié. Ce standard s'est beaucoup inspiré de la technologie Bluetooth existante à cette époque, et qui répondait officiellement à la dénomination 802.15.1. Il a été ensuite rectifié en 2006 en proposant une couche MAC efficiente et quatre couches physiques. Les deux couches basses de cette norme sont utilisées par de nombreuses implémentations propriétaires comme ZigBee [37], WirelessHART [38], SynkroRF [39], RF4CE [40] et ISA100 [41].

Le succès de cette norme a donné des idées qui font avancer les travaux sur cette technologie. D'autres groupes de recherche ont vu le jour, ils ont comme objectif l'amélioration et l'adaptation de cette norme pour les besoins de futures applications. Diverses corrections et des améliorations sont proposées, ce qui permet d'avoir des débits plus élevés, une sécurité améliorée, et des possibilités de *Ranging* ou mesure de distances pour la localisation. Une nouvelle version de la norme, a été achevée en 2011 [42], elle a renforcé l'implémentation du standard IEEE 802.15.4-2006 dans le monde industriel, en éliminant les ambiguïtés et en incluant des améliorations suite aux implémentations du standard IEEE 802.15.4-2006. Dans cette partie, nous présenterons donc la norme IEEE 802.15.4-2006.

1.2.2.2.1 Topologie d'un réseau IEEE 802.15.4

Le standard IEEE 802.15.4-2006 [36] [43] [44] définit les spécifications de la couche physique et de la couche *MAC*. Ce *WPAN* supporte deux types de noeud : **FFD** (*Full Function Device*) et **RFD** (*Reduce Function Device*). Les noeuds FFD implémentent toute la pile protocolaire d'IEEE 802.15.4-2006, ils peuvent jouer trois rôles différents :

- le **coordinateur du PAN** a la possibilité de construire son propre réseau auquel les autres noeuds peuvent s'associer. Il contrôle tout le réseau et il est unique,
- le **simple coordinateur** est un noeud qui fournit une multitude de services aux noeuds simples comme la synchronisation par la transmission des *Beacon*. Ce type de noeud n'est pas capable de construire son propre réseau et il doit être associé à un coordinateur du **PAN**,
- Un **noeud simple** représente un noeud qui est associé à un coordinateur ou un coordinateur du **PAN**.

Les noeuds de type **RFD** implémentent les fonctionnalités basiques nécessaires pour le fonctionnement de la pile protocolaire d'IEEE 802.15.4-2006. Ils sont chargés de l'acquisition des données à partir de l'environnement et du traitement des informations. Un noeud **RFD** ne peut communiquer qu'avec des noeuds **FFD**, alors que les noeuds **FFD** peuvent communiquer avec tout type de noeud.

Les noeuds de type **FFD** et **RFD** permettent de définir trois topologies de base : étoile, arbre et maillée. La topologie en étoile (cf. Figure 1.6) permet uniquement une communication à un saut ou à deux sauts. Pour une large zone de déploiement, cette topologie n'est pas satisfaisante, car la portée de l'émetteur est parfois trop limitée. Dans cette topologie, les noeuds de type **RFD** ou **FFD** sont connectés au noeud central (obligatoirement **FFD**). Chaque réseau doit contenir un coordinateur de **PAN** qui est indiqué par un identificateur unique. Ce type de topologie est utilisé dans les applications qui demandent un faible délai de latence.

La topologie maillée permet les communications multi-sauts pour un déploiement massif sur une zone plus large. Cette topologie est décentralisée, chaque noeud peut communiquer sans intermédiaire avec les noeuds qui sont dans sa zone de couverture radio (cf. Figure 1.7). Dans cette topologie, seuls des noeuds de type **FFD** sont déployés.

La topologie en arbre, plus rigide qu'un simple réseau maillé, offre également une couverture plus étendue avec la notion de la hiérarchie. Tous les noeuds de l'arbre sont des **FFD** sauf les feuilles qui sont des noeuds **RFD**. Les noeuds intermédiaires entre le sommet et les feuilles peuvent agir comme des coordinateurs et assurer la synchronisation entre les différents types de noeuds (soit un **FFD**, soit un **RFD**). Un seul noeud de ces coordinateurs peut être le coordinateur du **PAN** (cf. Figure 1.8). À l'aide d'une couche réseau et d'un protocole de routage (par exemple avec *ZigBee*), il est possible d'élaborer une topologie plus complexe qui contient les topologies élémentaires : arbre, maillé et

étoile (cf. Figure 1.9).

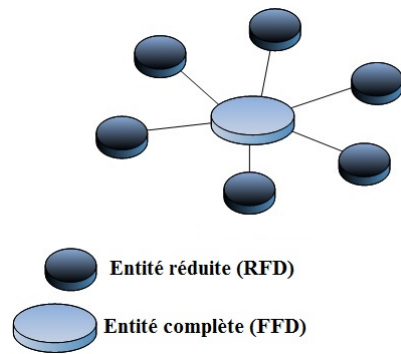


FIGURE 1.6: Topologie en étoile

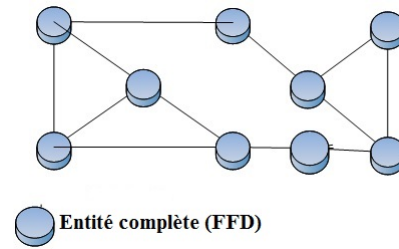


FIGURE 1.7: Topologie maillée

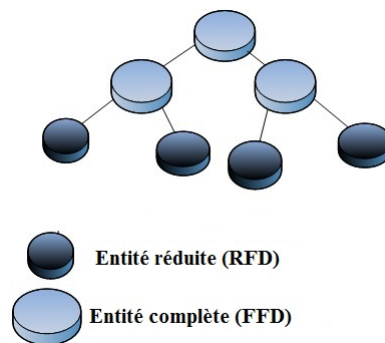


FIGURE 1.8: Topologie en arbre

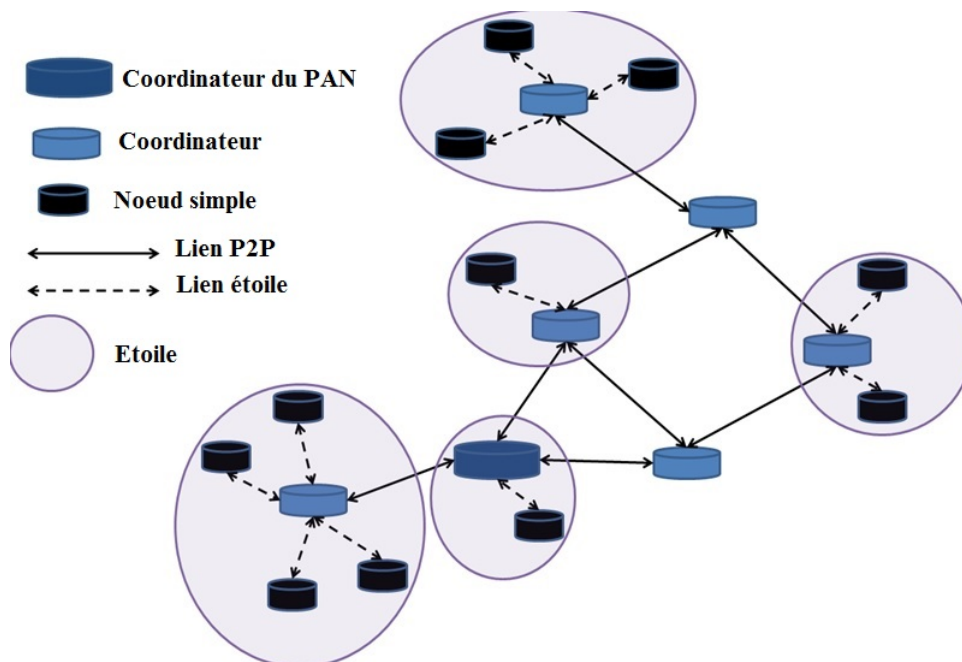


FIGURE 1.9: Topologie générale complexe

1.2.2.2.2 Modes de synchronisation de la norme IEEE 802.15.4

Dans la norme [IEEE](#) 802.15.4-2006, il existe deux modes de synchronisation (cf. Figure 1.10) :

- **avec beacon** : ce mode est par exemple utilisé dans les réseaux en étoile, où le coordinateur du réseau transmet des *beacons* périodiquement à chaque début d'une nouvelle supertrame [45, 46] (cf. Figure 1.11). Une supertrame est un intervalle de temps délimité par deux *beacons* et sa durée est déterminée par le coordinateur. Le *beacon* contient des informations de synchronisation et des informations sur les périodes dans lesquelles chaque nœud peut ou doit être dans l'état actif ou inactif.
- **sans beacon** : aucun *beacon* n'est émis dans cette configuration de réseau. Ce mode est utilisé par exemple avec l'architecture maillée où tous les nœuds de type [FFD](#) et l'accès au médium s'effectuent avec la méthode [CSMA/CA](#) (*Carrier Sense Multiple Access with Collision Avoidance*) non slotté.

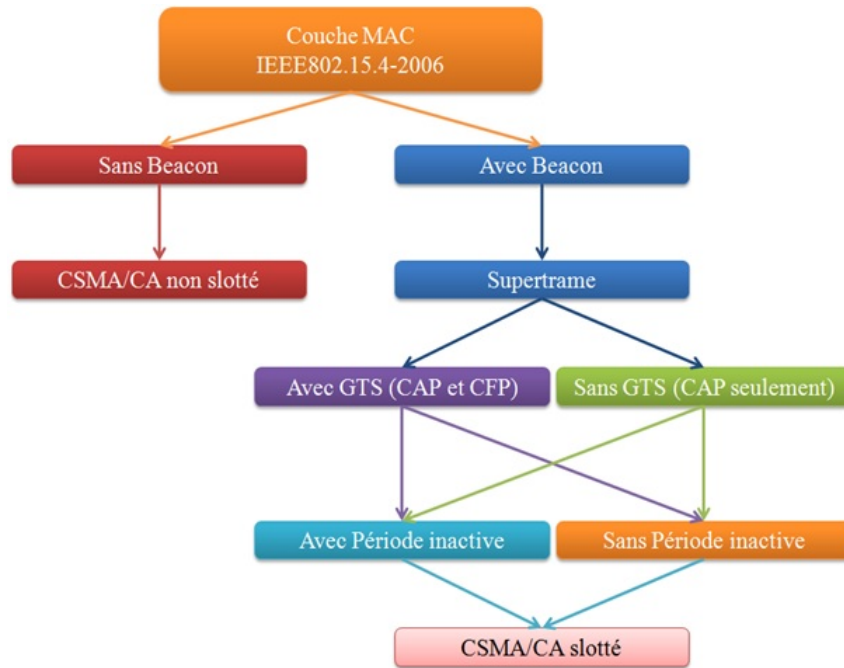


FIGURE 1.10: Modes d'exécution de la sous-couche MAC de la norme IEEE 802.15.4-2006

Dans la suite, nous allons nous intéresser au mode avec *beacon* où la communication entre les nœuds s'effectue pendant la durée de la supertrame.

L'utilisation de la supertrame, dans la norme [IEEE](#) 802.15.4-2006, est optionnelle (cf. Figure 1.10). Lorsqu'elle est utilisée, la structure de la supertrame est définie par le coordinateur de réseau. Elle est généralement composée de deux périodes de temps (cf. Figure 1.11 et Figure 1.10) : une période active et une période inactive.

Dans la période inactive, qui est optionnelle, le nœud est dans le mode veille. La durée de la période active, appelé aussi durée de supertrame [SD](#) (*Superframe Duration*) est

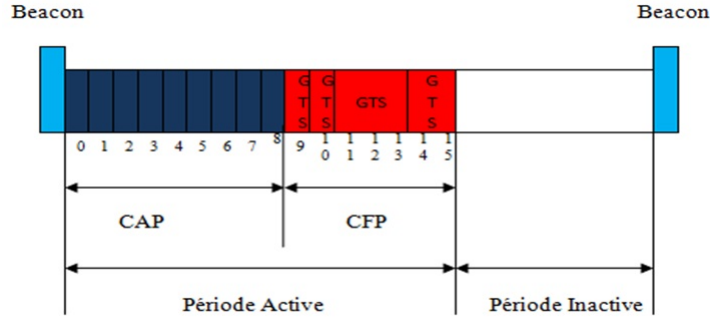


FIGURE 1.11: Structure d'une supertrame

calculée par :

$$SD = 960 \times 2^{SO} \text{ symboles} \quad (1.1)$$

La durée entre deux beacons successifs **BI** (*Beacon Interval*) est égale à :

$$BI = 960 \times 2^{BO} \text{ symboles} \quad (1.2)$$

Les valeurs de **SO** (*Superframe Order*) et **BO** (*Beacon Order*) sont déterminées par le coordinateur du réseau et doivent vérifier la condition suivante : $0 \leq SO \leq BO < 15$.

La période active est composée de seize slots de temps dont le premier est réservé pour le *beacon*. Cette période est divisée en deux parties : une période d'accès en période de contention ou **CAP** (*Contention Access Period*), et une période d'accès sans contention ou **CFP** (*Contention Free Period*).

Dans la période CAP, les nœuds utilisent le **CSMA/CA** slotté pour accéder au canal. Dans ce cas là malheureusement, le protocole d'accès **CSMA/CA** ne garantit pas une transmission totalement fiable entre les nœuds, car il existe un risque non nul de collisions entre des émissions simultanées de la part de nœuds concurrents. Les nœuds accèdent au canal aléatoirement et il n'est pas possible d'offrir aux nœuds un accès au canal sûr à 100%. Par contre, durant la période CFP, le coordinateur de l'étoile attribue à certains nœuds le privilège d'accéder au canal dans un intervalle de temps fixe (grâce à l'octroi d'un ou plusieurs **GTS** (*Guaranteed Time Slot*)).

Pendant cette période **CFP**, il n'y a qu'un seul nœud qui a le droit d'émettre ; il n'y aura donc pas de collision dans l'étoile. On peut considérer que dans cette période, les nœuds à qui ont été donnés des **GTS**, exploitent un protocole de type **TDMA** pour la transmission des données dans la période **CFP**.

Le nombre de slots de temps qui peuvent être alloués dans la **CFP** ne dépasse pas 7 dans la norme initiale. Tous les nœuds qui ont utilisé la période **CAP** doivent terminer leurs transmissions de données avant le début de la période **CFP**. De même, les nœuds qui ont réservé des **GTS** doivent terminer leur transmission avant le début d'un nouveau **GTS** ou la fin de la période **CFP** et donc de la supertrame.

La norme [IEEE](#) 802.15.4-2006 définit donc trois modes de transmission des données :

- **transmission directe** : ce mode de transmission est utilisé dans les réseaux de topologie étoile, il permet la transmission des données du coordinateur de l'étoile vers un nœud [RFD](#) et inversement. Les nœuds utilisent le [CSMA/CA](#) non slotté ou slotté selon le mode de synchronisation utilisé dans le réseau (respectivement sans et avec *beacon*),
- **transmission indirecte** : dans le réseau de capteurs, les nœuds ne peuvent pas rester dans l'état actif indéfiniment sauf pour la réception des données ou l'attente du *beacon* de la supertrame suivante. Lorsque le coordinateur de l'étoile transmet le *beacon*, chaque nœud [RFD](#) vérifie s'il a des messages en attente d'émission. Pour que les nœuds destinataires reçoivent les données en attente, ils envoient une demande au coordinateur de l'étoile,
- **Transmission à travers les [GTS](#)** : dans ce mode, les nœuds qui ont réservé des slots de temps sont les seuls autorisés à transmettre des données aux instants dédiés. Les données peuvent être transmises du coordinateur de l'étoile vers un autre nœud [RFD](#) ou inversement. Le [CSMA/CA](#) n'est pas utilisé dans ce mode.

Les transmissions directes et indirectes sont utilisées dans la période [CAP](#) uniquement, la transmission à travers les [GTS](#) est utilisée dans la période [CFP](#). La spécification au niveau de la couche MAC propose, également, un ensemble des services qui permettent de gérer la transmission des trames comme la *purge* qui offre la possibilité aux couches supérieures de supprimer une trame de la file d'attente de transmission avant qu'elle soit transmise. Nous exploiterons avantageusement cette fonctionnalité présentée ultérieurement.

1.2.2.2.3 Couche physique de la norme [IEEE](#) 802.15.4

Au niveau physique, la norme [IEEE](#) 802.15.4-2006 définit 27 canaux radio qui sont répartis sur trois bandes de fréquences :

- 16 canaux de fréquence pour la bande de 2.4 à 2.4835 GHz,
- 10 canaux de fréquence pour la bande 902 à 928 MHz,
- un canal de fréquence pour la bande 868 à 868.6 MHz.

De plus, elle spécifie quatre couches physiques dont deux sont optionnelles :

- **[ISM](#) 2.4 GHz** : elle offre la meilleure performance avec l'utilisation de l'étalement de spectre à séquence directe [DSSS](#) (*Direct Sequence Spread Spectrum*) et la modulation [O-QPSK](#) (*Offset Quadrature PSK*),

- **868 et 915 MHz** : la fréquence 868 MHz est définie pour une utilisation en Europe alors que la fréquence 915 est définie pour une utilisation en USA. Cette couche physique est basée sur le **DSSS** et utilise la modulation **BPSK** (*Binary Phase-Shift Keying*). Nous pouvons également avoir l'utilisation de **DSSS** avec la modulation **O-QPSK** à la place de **BPSK**, mais aussi l'utilisation de **PSSS** (*Parallel Sequence Spread Spectrum*) avec **BPSK**. Ceci permet ainsi d'avoir trois couches physiques différentes dans la même bande de fréquence.

1.2.2.2.4 Amendements de IEEE 802.15.4

Plusieurs travaux ont été effectués sur la norme **IEEE 802.15.4**, ils ont donné lieu à l'apparition d'autres normes qui proposent des améliorations et des corrections à la norme de base :

- **IEEE 802.15.4a** : publié en 2007, cette norme propose deux nouvelles couches physiques qui utilisent : l'**UWB** et le **CSS** (*Chirp Spread Spectrum*) (utilisé par exemple pour le Ranging [47, 48]),
- **IEEE 802.15.4b** : elle propose des améliorations et des clarifications spécifiques à la version **IEEE 802.15.4-2003**, telles que la réduction du niveau de complexité et l'augmentation de la flexibilité [49],
- **IEEE 802.15.4c** : publiée en 2009, elle définit les spécifications techniques d'une nouvelle couche *PHY* alternative aux standards **IEEE 802.15.4-2006** et **IEEE 802.15.4a**. Cette couche utilise les bandes 314 MHz-316 MHz, 430 MHz-434 MHz et 779 MHz-787 MHz [49],
- **IEEE 802.15.4d** : publiée en 2009, elle définit les spécifications techniques d'une nouvelle couche physique qui opère dans la bande 950 MHz -956 MHz [49],
- **IEEE 802.15.4f** : publiée en 2012, elle définit deux nouvelles couches physiques pour les systèmes **RFID** (*Radio Frequency Identification Device*) actifs dans les bandes 2.4 GHz, 433 MHz (couche physique **MSK** (*Minimum Shift Keying*)) et **UWB** (couche physique **LRP-UWB** (*Low Rate Pulse repetition frequency UWB*)) [49],
- **IEEE 802.15.4g** : publiée en 2012, elle définit de nouvelles couches physiques pour les réseaux à voisinages intelligents. Cette norme propose des changements à effectuer sur la norme **IEEE 802.15.4-2011** [49],
- **IEEE 802.15.4j** : cette norme définit une nouvelle couche physique, et opère dans la bande 2360 MHz-2400 MHz, pour le standard **IEEE 802.15.4** qui est conforme aux exigences des **MBAN** (*Medical Body Area Network*) [49],
- **IEEE 802.15.4k** : cette norme définit une nouvelle couche physique qui facilite les communications point-multipoints pour le cas des infrastructures critiques de dispositifs de surveillance [49],

- **IEEE 802.15.4-2011** : cette norme est une amélioration de la version 2006, elle intègre les améliorations suite aux implémentations du standard IEEE 802.15.4-2006 comme la norme IEEE 802.15.4a qui offre un débit très intéressant avec l'utilisation de la technologie *UWB* [49].

Dans cette partie, nous avons présenté la norme IEEE 802.15.4-2006. Le groupe 802.15 ne cesse d'améliorer et d'augmenter le nombre de sous-groupes afin d'être capable de suivre et de répondre aux besoins et aux exigences des applications récentes et futuristes. Être toujours au centre des avancées technologiques et applicatives est un objectif qui n'est pas simple à atteindre. Mais, ceci représente pour le groupe 802.15 une motivation qui s'est concrétisée par l'apparition de plusieurs normes, en particulier le dernier né de cette fameuse famille : IEEE 802.15.6. Bien que la norme IEEE 802.15.4 et la norme IEEE 802.15.6 appartiennent à la même famille, elles sont finalement assez concurrentes.

1.2.2.3 La norme IEEE 802.15.6-2012

Un nouveau groupe, au sein de l'IEEE 802.15 [50] a été créé sous le nom *TG6* (*Task Group 6*) en 2007 [51] pour proposer une nouvelle technologie pour les communications à faible consommation d'énergie et à faible portée pour les applications *e-health*.

1.2.2.3.1 Type de nœud et technologie physique

Dans la première version proposée de la norme IEEE 802.15.6 [52], en 2009, trois types de nœuds sont définis :

- **le nœud implant** : c'est un nœud placé à l'intérieur du corps humain. Il peut être par exemple au dessous de peau ou dans les veines,
- **un nœud à la surface du corps** : c'est un nœud placé sur la surface de la peau humaine. Ce dernier ne peut pas être éloigné de plus de deux centimètres de la peau,
- **le nœud externe** : c'est un nœud qui n'est pas en contact avec la surface de la peau du corps et qui n'est pas plus loin de 5 mètres.

Ces trois types de nœuds permettent de réaliser 5 scénarii différents de communication [52] (cf. Figure 1.12) :

- **scénario 1** : implant avec implant,
- **scénario 2** : implant avec un nœud à la surface du corps,
- **scénario 3** : implant avec un nœud externe,

- **scénario 4** : un nœud à la surface du corps et un autre nœud en surface d'un autre corps (avec le mode **LOS** (*Line Of Sight*) ou **NLOS** (*Non Line of Sight*)),
- **scénario 5** : un nœud à la surface du corps et un nœud externe (avec le mode **LOS** ou **NLOS**).

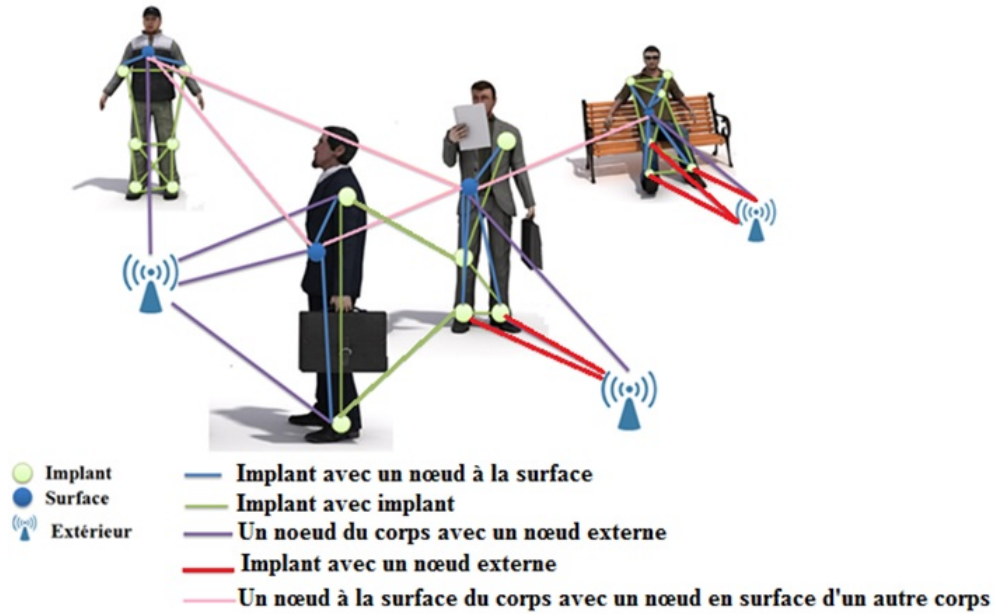


FIGURE 1.12: Les différents scénarii présentés dans la norme IEEE 802.15.6

Dans les scénarii proposés, nous retrouvons des communications passant par des milieux ou médiums différents. Cette variation de milieux influence énormément la qualité des liens, et induit une augmentation du taux d'erreur bits BER. Une autre exigence importante est liée à la puissance maximale du signal, définie par le **MICS** (*Medical Implant Communications Service*), qui ne doit pas dépasser 2.2 dBm.

Pour chaque scénario, la norme **IEEE** 802.15.6-2006 a défini une bande de fréquences précise (cf. Tableau 1.1). Nous avons donc trois couches différentes qui permettent la

Scénario	Bande de fréquence
1	402-405 MHz
2	402-405 MHz
3	402-405 MHz
4	13.5, 50, 400, 600, 900 MHz 2.4, 3.1-10.6 GHZ
5	13.5, 50, 400, 600, 900 MHz 2.4, 3.1-10.6 GHZ

TABLE 1.1: Différents scénarii associés à des bandes de fréquences adéquates

communication entre trois types de nœuds [53, 54] :

- **NB** (*Narrow Band*) : utilisé par les nœuds qui opèrent dans la bande de fréquences des **MBAN** comme les implants et les capsules endoscopiques,

- **UWB** : utilisé par les nœuds qui ont besoin d'un débit élevé. Deux technologies radio différentes sont définies : **IR-UWB** (*Impulse Radio UWB*) et **FM-UWB** (*Frequency Modulated UWB*),
- **HBC** (*Human Body Communication*) : pour les communications sur la surface de corps humain.

1.2.2.3.2 Topologies définies

La norme IEEE 802.15.6 se base sur une topologie étoile et sur la topologie en arbre avec profondeur deux au maximum (il peut y avoir 4 sauts) (cf. Figure 1.13). Dans la topologie en étoile, l'échange des messages s'effectue entre un nœud appelé *hub* et un nœud normal. Dans le cas de l'arbre, le nœud intermédiaire entre l'*hub* et un autre nœud jouent le rôle d'un relais. Le TG6 recommande l'utilisation des topologies hybrides et maillées [50] (cf. Figure 1.14). Le nombre maximal de nœuds supporté par le *hub* d'un réseau BAN est de 64.

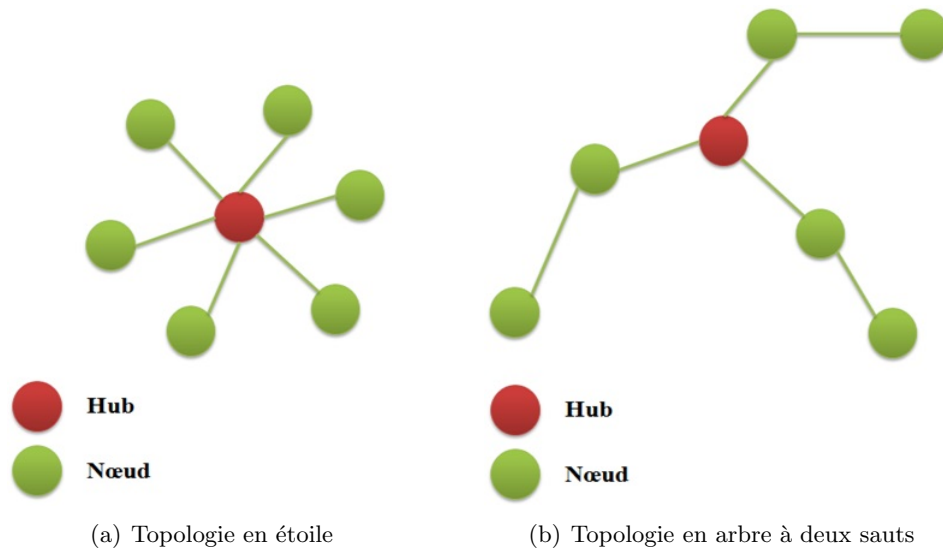


FIGURE 1.13: Topologies utilisées dans la norme IEEE 802.15.6

Le nœud *hub* est unique dans le réseau BAN et responsable de la coordination de l'accès au canal. Il divise le temps en périodes appelées supertrames, ou périodes de *beacon*. Le *hub* émet des *beacons* dans chaque supertrame sauf dans le cas des supertrames inactives où les *beacons* ne sont pas utilisés.

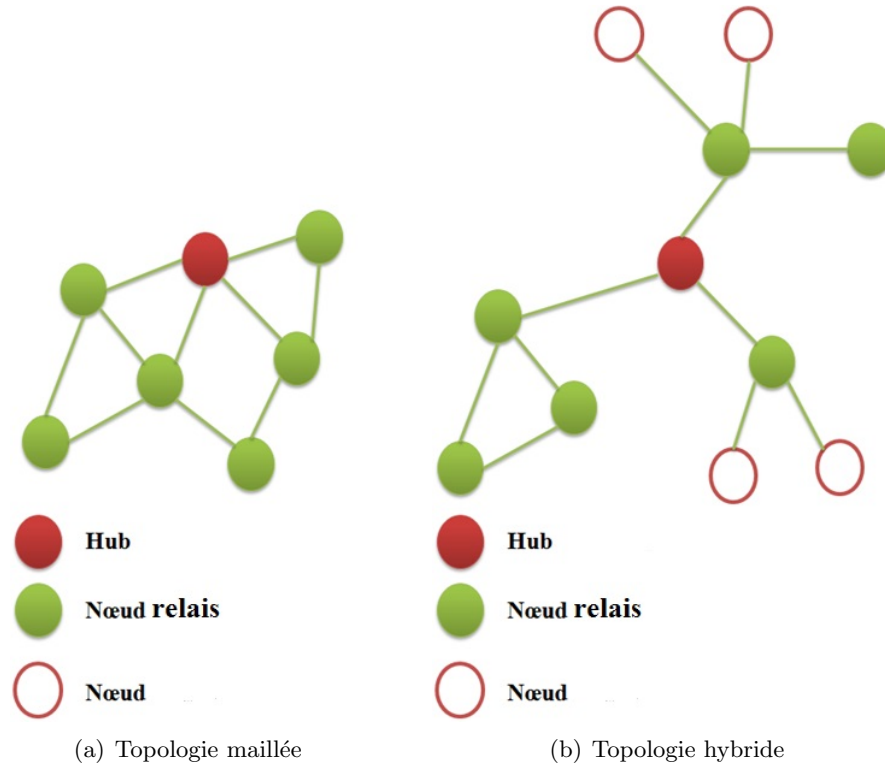


FIGURE 1.14: Topologies recommandées par la norme IEEE 802.15.6

1.2.2.3.3 Gestion du réseau

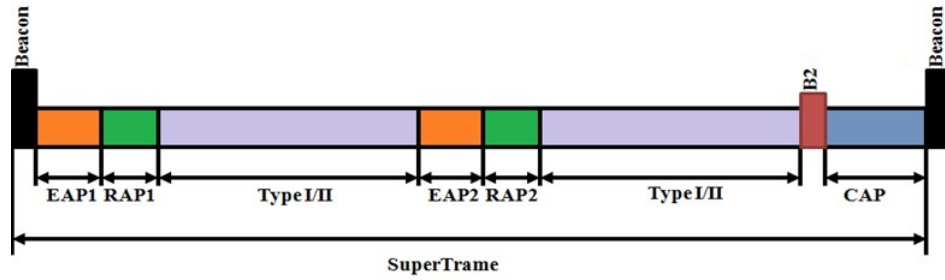
Le *Hub* peut choisir l'un des trois modes suivants pour la gestion de réseau *BAN* :

- avec *beacon* et avec supertrame,
- sans *beacon* et avec supertrame,
- sans *beacon* et sans supertrame.

La Figure 1.15 présente la structure d'une supertrame dans le mode avec *beacon* et avec supertrame. Cette dernière est délimitée par deux *beacons*. Au début de chaque supertrame, nous retrouvons un *beacon* suivi par deux périodes successives. Chaque période contient trois sous-périodes : *EAP* (*Exclusive Access Phase*), *RAP* (*Random Access Phase*) et Type I/II (appelée aussi *MAP* (*Managed Access Phase*)) consécutivement. Après ces deux périodes, nous pouvons avoir une trame B2, qui précède la période *CAP*, qui indique que la période *CAP* est non nulle [55, 56]. La trame B2 est optionnelle.

La durée des différentes périodes dans la supertrame est variable et leurs longueurs sont données en fonction du nombre de slots réservés. La structure de la supertrame peut être modifiée en désactivant des périodes définies [55, 57].

Les périodes *EAP1* et *EAP2* sont réservées pour les trafics à haute priorité comme les messages d'urgence. Les périodes *RAP1*, *RAP2* et *CAP* sont réservées pour les trafics

FIGURE 1.15: Composition de la supertrame dans le mode avec *beacon*

réguliers alors que les périodes Type I/II sont prévues pour la réservation des périodes de transmission ou la transmission des trafics imprévus. Les nœuds qui ont des réservations de Type I/II commencent la transmission des messages lorsque leurs périodes réservées débutent. Les nœuds qui utilisent l'accès imprévu doivent rester actifs. Ces nœuds peuvent commencer la transmission de leurs messages lorsqu'ils reçoivent une trame *Poll* ou *Post* envoyée par le *hub*. Les accès Type I et Type II ne peuvent pas être mélangés dans chaque période Type I/II parce que ces deux types ont une différence au niveau de l'unité utilisée dans la demande de réservation : pour le Type I, le nœud envoie une demande de réservation de période de transmission en fonction du temps demandé alors que pour le Type II, la période demandée est en fonction du nombre de trames [57], [55], [56]. Dans ce mode, existent trois types d'accès qui sont définis pour chaque période :

- **accès aléatoire** : dans cette méthode d'accès, le nœud utilise la technique CS-MA/CA ou ALOHA slotté pour accéder au médium dans les périodes EAP1, EAP2, RAP1, RAP2 et CAP avec l'utilisation de la couche physique NB ou UWB respectivement,
- **accès improvisé et imprévu** : les nœuds qui utilisent cette méthode transmettent leurs messages dans les périodes Type I/II après la réception d'une trame *Post* ou *Poll* du *hub*. La trame *Post* est utilisée lorsque le *hub* transmet les trames alors que la trame *Poll* est utilisée pour que le nœud commence la transmission,
- **accès prévu** : dans ce type d'accès, la réservation de période de transmission peut être dans chaque supertrame (*1-periodic*) ou dans chaque m supertrames (*m-periodic*), ce qui permet de plus au nœud d'entrer dans le mode *Sleep* entre deux périodes de transmission.

Dans le mode sans *beacon* avec supertrame, la supertrame entière est utilisée par la période d'accès Type I ou Type II. Afin d'informer les nœuds des limites de la supertrame ; le *hub* utilise la trame *T-poll* [56].

Dans le dernier mode sans *beacon* et sans supertrame, seule la réservation imprévue pour le Type II est autorisée. Ce mode supporte l'existence d'une période CAP [57]. Dans ce mode, le *hub* peut envoyer les trames *Post* et *Poll* à n'importe quel moment [56].

La norme [IEEE 802.15.6-2012](#) est nativement désignée pour les applications médicales. Pour satisfaire les exigences de ce domaine, différents niveaux de priorité ont été introduit afin d'assurer la bonne gestion de trafics selon l'importance de l'information (cf. [Tableau 1.2](#)).

Priorité	Priorité de l'utilisateur	Trafic associé	Type de trame
Faible	0	BK	Donnée
	1	BE	
Moyenne	2	EE	Donnée ou Gestion
	3	VI	
	4	VO	
	5	Donnée médicale ou de contrôle	
	6	Donnée médicale à forte priorité ou de contrôle	
Forte	7	Rapport de cas d'urgence	Donnée
		ou d'un implant	

TABLE 1.2: Priorités associées à chaque type de trafic [57]

La norme [IEEE 802.15.6](#) est dédiée aux applications médicales et non médicales. Elle utilise des technologies qui sont définies dans [IEEE 802.15.4-2011](#) à l'exception de [HBC](#). Les points forts de cette technologie face à [BLE](#) et [IEEE 802.15.4](#) résident dans la définition d'un nouveau type de nœud (les implants) et la définition des priorités au niveau MAC, ce qui simplifie la tâche d'implémentation. Mais, il reste plusieurs points ambigus qui demandent de nombreuses améliorations futures. Il n'existe à ce jour aucun matériel qui implémente la technologie [IEEE 802.15.6](#) et les applications médicales qui sont développées en ce moment se basent essentiellement sur la norme [IEEE 802.15.4](#). Cette dernière s'améliore rapidement et plusieurs groupes sont créés pour l'adapter aux structures d'urgence, à [IPV6](#)... Ceci nous amène à nous poser des questions sur le futur de cette nouvelle norme : d'autres groupes travailleront-ils sur l'amélioration et la correction des problèmes existants, ou sera-t-elle intégrée dans la nouvelle version d'[IEEE 802.15.4](#) ?

Bien que l'avenir de cette technologie ne soit pas encore très clair, son architecture et ses solutions restent majeures. Elle se présente donc également comme une candidate potentielle pour les applications [WBAN](#) et en particulier les applications du futur.

1.2.2.4 ANT : Advanced and adaptive Network Technology

Le développement de nouvelles méthodes d'accès pour les applications *e-santé* ne se limite pas à des organismes connus comme [IEEE](#). Les entreprises cherchent également à trouver des solutions propriétaires et performantes qui les permettent de gagner cette bataille technologique et commerciale, et gagner de nouvelles parts de marché.

Dans cette partie, nous présentons la technologie [ANT](#) et son extension ANT+ [24], développées par Dynastream Innovations, qui sont considérées par la communauté industrielle comme les plus adaptées aux applications de surveillance dans les domaines qui nécessitent l'utilisation de réseaux de capteurs, en particulier pour le domaine sportif ou de la domotique.

1.2.2.4.1 Notion de *Master* et *Slave*

Le protocole [ANT](#) [P2] est classifié parmi les protocoles à faible consommation d'énergie. Il utilise la bande de fréquence 2,4 GHz [ISM](#) et il définit 125 canaux de largeur 1 MHz. Ceci lui permet d'atteindre un débit de 1 Mbits/s avec une durée de transmission égale à 150 μ s/trame pour 8 octets de données.

Dans la spécification [ANT](#) [P2], deux types de nœuds sont définis : *Master* et *Slave*. Le nœud *Master* est l'initiateur de la communication, le responsable de la gestion du canal et le transmetteur des données. La fenêtre de réception d'un nœud *Master* est utilisée pour permettre la coexistence de plusieurs maîtres qui utilisent la même fréquence dans le même réseau. Elle est utilisée, également, pour la réception des données provenant des *Slaves* ou d'autres *Masters* (cf. Figure 1.16).

Le nœud *Slave* est le récepteur principal des trames de données et le responsable de la synchronisation avec le *Master* (cf. Figure 1.16).

Dans le protocole [ANT](#) [P2][P4], un nœud peut agir comme un *Master* et un *Slave* en même temps selon le type de communication établie avec les nœuds de réseau. Par exemple, dans la Figure 1.16, nous identifions trois nœuds où le nœud 1 est le *Master* du nœud 2 qui joue le rôle d'un *Slave* dans ce cas, alors que le nœud 3 est le *Master* du nœud 1 (*Slave*).

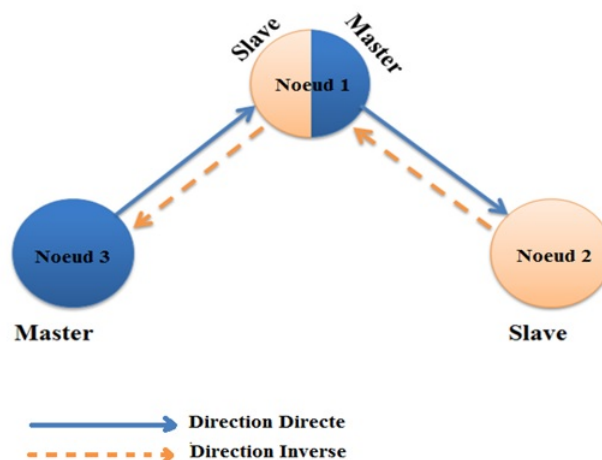


FIGURE 1.16: Les différents rôles joués par un nœud ANT

1.2.2.4.2 Paramètres de connexion

Afin de créer une connexion entre deux nœuds, ces derniers doivent avoir la même configuration de canal. Le nœud *Slave* doit connaître les paramètres [24] :

- **réseau** : le protocole [ANT](#) peut créer différents types de réseaux : publics et privés. Pour que deux nœuds puissent échanger des messages, ils doivent être dans le même réseau. Afin d'assurer la confidentialité et limiter l'accès, [ANT](#) permet la création d'un réseau privé,
- **fréquences RF** : ce paramètre représente la fréquence dans laquelle opère le réseau. Par exemple, si la valeur de ce paramètre est égal à 66, cela signifie que les nœuds utilisent la fréquence 2466 MHz,
- **ID de canal** : c'est la plus importante information pour les nœuds. Ce paramètre est spécifié par les couches supérieures. Sa valeur est codée sur 4 octets qui permettent de définir les informations suivantes :
 - **type de transmission** : codé sur 8 bits,
 - **type de nœud** : codé sur 8 bits, ce paramètre est utilisé pour annoncer le type de nœud. Ceci permet aux nœuds participants à la connexion de connaître le type des nœuds connectés, donc de connaître leurs classes. Ceci permet le décodage des informations reçues. Si le nœud est de type 0 alors le nœud récepteur peut établir une connexion avec plusieurs types de nœuds,
 - **numéro de nœud** : codé sur 16 bits, il est unique dans le réseau.
- **type de canal** : il définit le type de transmission utilisé. Cette information est codée sur 8 bits ce qui permet d'avoir 8 types de transmission,
- **période de canal** : codée sur 16 bits. Elle représente la période de base utilisée par le *Master* pour la transmission des données. La fréquence de transmission des trames de données qui en découle varie entre 0,5 Hz et 200 Hz, la valeur par défaut est égale à 4 Hz (cf. Figure 1.17),
- **format et type de données** : ceci détermine le type de communication établi entre les nœuds participant. Ce paramètre est fixé par les couches supérieures [58] :
 - **gestion de la direction** (cf. Figure 1.18) :
 - * direction directe (du *Master* vers le *Slave*),
 - * direction inverse (du *Slave* vers le *Master*).
 - **spécification du type de la communication** :
 - * diffusion,
 - * acquittement,
 - * rafale.

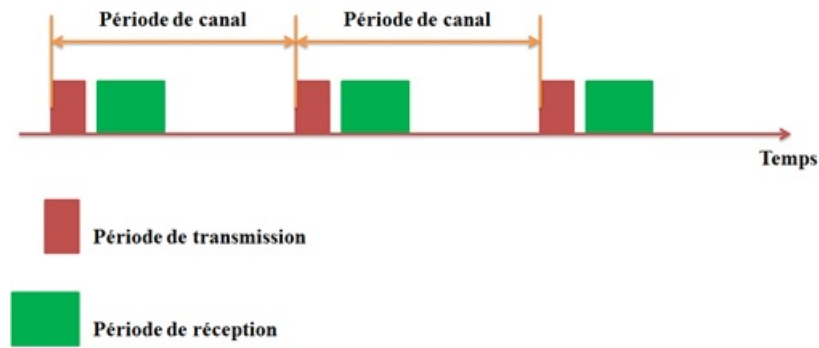


FIGURE 1.17: Les périodes de canal de ANT

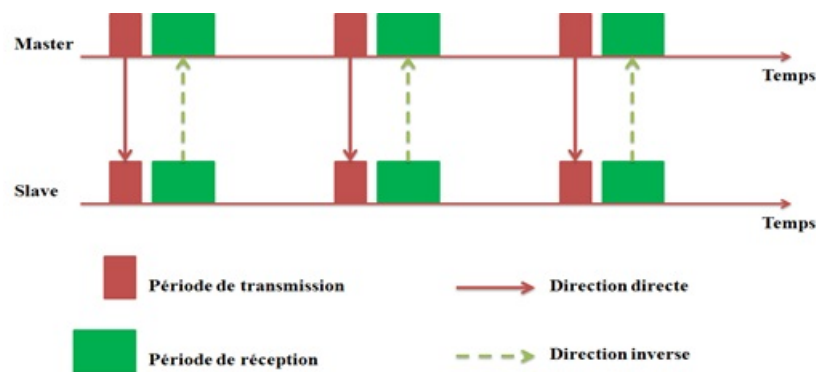


FIGURE 1.18: La gestion de la direction de ANT

1.2.2.4.3 Processus d'établissement de connexion

Trois types de canaux sont définis : des canaux indépendants, des canaux partagés et des canaux de balayage ou *scan*.

Dans les canaux indépendants, existent un *Master* et un *Slave* seulement. Les nœuds peuvent jouer d'autres rôles dans d'autres canaux et le nombre de canaux indépendants supportés est illimité.

Les nœuds utilisent les canaux de partage et de balayage dans le cas de réception des données de plusieurs sources. Dans le mode balayage, le nœud *Slave* reste à l'écoute tout le temps. Pour cette raison, il reçoit des messages de plusieurs *Masters*. Le nœud *Slave* ne peut pas créer une communication avec d'autres nœuds, car sa radio est toujours dans l'état de réception.

Afin d'établir une communication entre deux nœuds, la spécification d'[ANT](#) définit un ensemble d'états qui doivent être respectés : en premier, le *Master* définit l'ensemble des paramètres nécessaires pour l'établissement de la connexion. Il définit ensuite un canal pour la transmission de l'identifiant de ce dernier dans des intervalles de temps précis (période de canal). Ce canal sera maintenu avec la même fréquence de transmission et le même débit. Afin que la transmission des trames ne s'arrête pas, les couches supérieures fournissent de nouvelles données aux couches inférieures. Puis, le *Slave* active sa radio pour chercher un *Master* spécifique ou un sous-ensemble de *Masters*. Dès qu'il reçoit le

premier message du *Master* demandé, il sélectionne le type de réseau, la fréquence et la vitesse de transmission. Avec ces informations, il peut se synchroniser avec le *Master* et recevoir les données [59], [60], [61].

1.2.2.4.4 Couches supérieures de ANT : ANT+

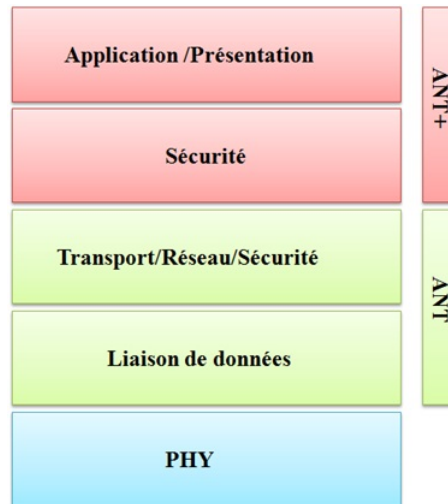


FIGURE 1.19: Pile protocolaire ANT/ANT+

Le protocole [ANT](#) spécifie essentiellement les couches liaison de données, réseaux et transport. Les couches supérieures sont définies dans la spécification de ANT+ (cf. Figure 1.19) qui simplifie la collection, le suivi et la transmission des informations sur la santé de la personne surveillée. Cette couche assure l'interopérabilité dans le réseau et définit la structure des messages utilisés.

ANT+ rend le partage d'un canal entre plusieurs participants possible. Il s'occupe de la gestion des définitions des profils des nœuds afin de connaître les besoins des nœuds participants.

La technologie [ANT](#) présente plusieurs avantages pour les applications *e-santé*. Elle est dédiée essentiellement à la communication entre des capteurs de collecte d'informations et un nœud plus puissant comme un Smartphone, qui reçoit l'information afin de la transférer sur un outil de traitement ou la présenter directement à l'utilisateur.

Dans la partie suivante, nous discuterons des points forts et des points faibles de chaque technologie présentée. L'objectif de cette discussion est d'identifier la technologie la plus adaptée pour être utilisée dans le projet *CANet* et de mettre en évidence les possibilités de coopérations entre les différentes technologies dans le cas de l'existence de plusieurs types d'applications pour ce même projet.

1.2.2.5 Discussion

La présence de plusieurs technologies qui peuvent réaliser les mêmes fonctions rend le choix entre elles difficile. Pour cette raison, la comparaison s'impose. La technologie choisie doit être la plus adaptée à notre projet de thèse qui s'articule sur le domaine de surveillance présenté par le projet *CANet*, en particulier la surveillance des personnes âgées. Nos candidats précédemment présentés sont : [BLE](#), [IEEE 802.15.4](#), [IEEE 802.15.6](#) et [ANT](#). Ils sont connus par la communauté scientifique et industrielle. Certaines de ces technologies sont déjà utilisées et offrent des services et des applications pertinentes pour l'utilisateur.

La technologie [BLE](#) offre un débit important et suffisant pour les applications [BAN](#). Le point fort de cette technologie est son interopérabilité puisqu'elle est compatible avec *Bluetooth* [BR/EDR](#) et qu'elle est utilisée à large échelle, essentiellement dans les ordinateurs portables et les *Smartphones*. Malheureusement, cette technologie supporte mal les transmissions en temps réel, et souffre d'une faible taille de données que les paquets peuvent supporter, qui ne dépassent pas 48 octets. Cette technologie est plus adaptée aux transmissions des données périodiques qui tolèrent une certaine latence.

Le standard [IEEE 802.15.4](#) est un candidat très connu dans l'environnement industriel et universitaire. Cette norme est très versatile au niveau de la couche *PHY*, en particulier la version 2011 qui propose la couche *PHY* [UWB](#) et les améliorations proposées par la norme [IEEE 802.15.4j](#) qui s'adresse spécialement au besoin du domaine médical au niveau de communication. Actuellement, [IEEE 802.15.4j](#) est la seule spécification pour la communication médicale qui réserve un nouveau spectre [MBAN](#) où le [BAN](#) peut opérer en réduisant considérablement les risques d'interférences [62].

Dans la norme [IEEE 802.15.6](#) nous trouvons, en particulier, plus de détails et de spécificités sur le réseau à proximité du corps humain, en particulier les implants et la possibilité de supporter une forte exigence de [QoS](#) pour les applications médicales et non médicales. La diversité des couches physiques définie dans la norme lui permet de s'adapter à plusieurs applications. La définition de différents niveaux de priorités qui sont associés à des périodes de transmission dans la supertrame, et la facilité de transmission de données via des trames improvisées lui donnent un avantage certain par rapport à [BLE](#) [62]. Malheureusement, le fait que la structure de la supertrame soit construite et basée sur la supertrame définie dans la norme [IEEE 802.15.4](#) rend cet avantage caduque. D'autre part, la limitation à une topologie étoile représente un point faible par rapport à [IEEE 802.15.4](#).

Dans [63], les auteurs ont comparé [BLE](#) et [IEEE 802.15.4](#). L'étude théorique de [BLE](#) a montré que le débit offert est supérieur de 70% à celui de [IEEE 802.15.4](#). Dans la pratique, [BLE](#) offre un débit qui ne dépasse pas 123 kbit/s, qui est ainsi inférieur de 20 % au débit offert par [IEEE 802.15.4](#), proche de 190 kbit/s [63]. Les auteurs ont remarqué que les besoins de ressource pour la technologie [BLE](#) sont plus importants ceux imposés par [IEEE 802.15.4](#).

Finalement, les auteurs ont conclu que les limites de **BLE** par rapport aux autres technologies sont essentiellement au niveau de la radio de l'émission, la réception et la pile protocolaire qui ont besoin de plusieurs améliorations et corrections afin d'atteindre le débit et la latence minimale présentés dans les études théoriques. Dans cette étude, les auteurs ont utilisé la couche physique **ISM 2.4** de la norme **IEEE 802.15.4**, avec la technique **DSSS** qui permet d'atteindre un débit maximal égal à 250 kbit/s théoriquement. Ce débit est de 167.6 kbit/s et 189.5 respectivement avec l'utilisation des acquittements et sans acquittement [64] en **CSMA/CA**. Les auteurs n'ont pas comparé **BLE** aux nouvelles couches physiques 802.15.4 proposées dans la version 2011 qui permettent d'atteindre un débit supérieur ou égal à 1000 kbit/s. Cette dernière offre donc un débit largement supérieur à ceux de **BLE**.

Dans [65], les auteurs décrivent l'avenir des technologies sans fil sur la base de l'histoire de *Bluetooth* et de *Wifi* qui a commencé par un affrontement entre les deux standards et qui se termine actuellement par une coopération afin d'assurer un confort technologique fort pour les utilisateurs. Les auteurs pensent que dans le futur, nous aurons une coopération entre les architectures basées sur la norme **IEEE 802.15.4** et *Bluetooth*. Cette vision se résume dans la figure 1.20 où la technologie **BLE** est utilisée avec les applications *Smartphone* et la technologie **IEEE 802.15.4**, en particulier *Zigbee* et *Google's Thread*, est utilisée essentiellement pour les applications liées au concept de maison intelligente.

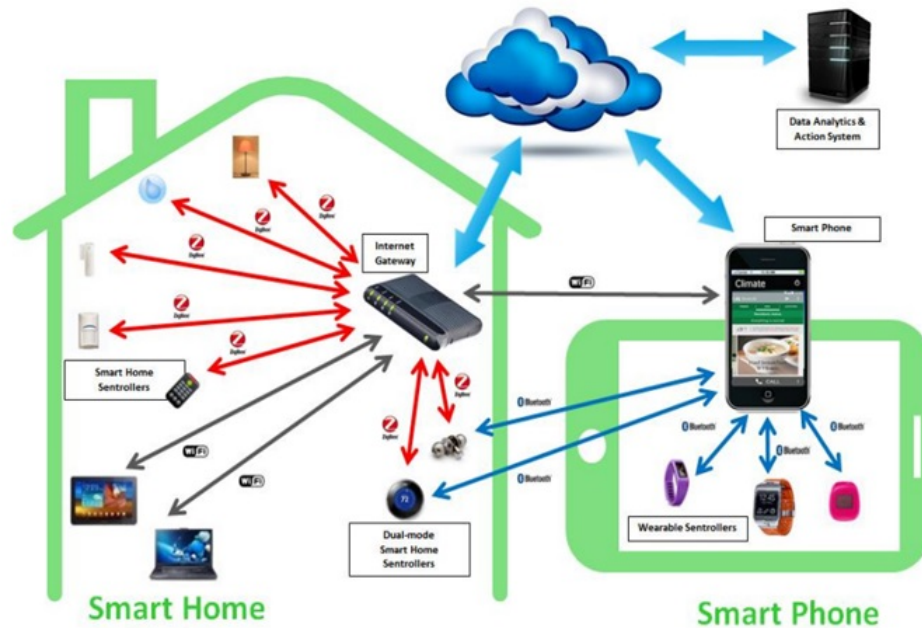


FIGURE 1.20: Utilisation de BLE, Wifi et Zigbee dans les applications de maison intelligente et de Smartphone [64]

La technologie **ANT** offre des performances équivalentes à celle de **BLE** et **IEEE 802.15.4**, mais le fait qu'elle soit une technologie non standardisée et propriétaire la désavantage. La méthode d'accès utilisée par **ANT** est proche de celle utilisée par **BLE**. A son avantage, **ANT** ne présente pas les problèmes inhérents à **BLE** comme les problèmes liés à l'utilisation de l'**AFH**. L'industrie a commencé à adapter **ANT** via son intégration dans

plusieurs produits. Cela nous ramène à mettre [ANT](#) et [BLE](#) sur le même niveau d'intérêt, si on omet le fait que [ANT](#) est une technologie propriétaire, qui n'est pas comme [BLE](#) soutenue par les grands acteurs économiques du monde des *Smartphones* même si on la trouve sur certains téléphones. Les technologies [IEEE 802.15.6](#) et [IEEE 802.15.4](#) restent plus intéressantes pour les applications qui nous concernent car elles offrent une diversité au niveau des couches physiques et des mécanismes d'accès au médium qui permet de limiter le nombre de collisions.

Le Tableau 3 représente un résumé des points les plus importantes pour choisir le meilleur candidat parmi ceux considérés pour les applications [BAN](#).

Type de nœud ou rôle		802.15.4		802.15.6	BLE	ANT
		2006	2011			
Architecture possible		RFD et FFD		Hub et Nœud ordinaire	Master et Slave	Master et Slave
Couche Liaison des données	Mécanisme d'accès	Etoile, arbre, maillée, hybride		Etoile, arbre	Etoile (Piconet)	Maillée, étoile, arbre
		TDMA	TDMA	CSMA/CA ALOHA	TDMA	TDMA
	Taille de la trame (octets)	CSMA/CA	CSMA/CA ALOHA			
	Control d'erreur	127		255	8 à 47	8
Identification		ARQ			24-bit CRC. ACK	16-bit CRC
Couche Physique		16 et 64 bits d'adresse MAC	Identificateur de taille 8 bits		48 bits d'adresse Bluetooth ou une adresse aléatoire	-
	Bande RF (MHz)	868-868,6 902-928 2400-2483,5	779-787 868-868.6 902-928 950-956 2400-2483.5 250-750* 3244-4742* 5944- 10234*	402-405 420-450 863-870 2360-2400 2400-2483	2400	2403-2480
	Débit (Kbits/s)	20, 40, 250	20, 40, 100, 250, 1000, 110-27400	75.7-971.4, 202.5-15.600, 164-1312.5	1000	1000
	Modulation	BPSK, O-QPSK	BPSK, O-QPSK, ASK, GFSK, DQPSK, BPM, MPSK	DBPSK, DQPSK, D8PSK	GFSK	GFSK

Couche Physique	Technique d'étalement	802.15.4		802.15.6	BLE	ANT
		2006	2011			
		DSSS	DSSS, PSSS, CSS, UWB	NB, UWB, HBC	FHSS, AFH	FHSS
Zone de couverture (mètre)		10 – 30, 10-100 (2.4 GHz)	65.535	< 10	10 – 30	1 – 30
Taille de réseau					illimité	64.000
Trafic temps réel		GTS		EAP et 8 niveaux de priorité	Non	Non

TABLE 1.3: Comparaison entre les 4 principales technologies étudiées

Remarque

- * : Optionnelle,
- Couleur rouge : n'est pas bonne,
- Couleur vert : bonne.

La norme [IEEE 802.15.4](#) offre un débit comparable et même supérieur à ceux de 802.15.6 et [BLE](#). L'utilisation de la technologie TDMA, qui assure la transmission sans compétition dans les périodes GTS, rend la technologie [IEEE 802.15.4](#) capable de transmettre différents types de messages avec des niveaux de priorité et des exigences différentes.

L'utilisation de [TDMA](#) et [CSMA/CA](#) en même temps, avec l'ajout d'*ALOHA* dans la version 2011, donne à [IEEE 802.15.4](#) un avantage fort puisqu'il offre une base de différenciation entre les trafics, ce qui peut induire des résultats très performants dans le cas d'une forte diversité des paramètres et d'exigences des matériels médicaux. Tous ces points rendent le standard [IEEE 802.15.4](#) le plus adapté pour son utilisation dans les applications de surveillance.

Finalement, nous pouvons conclure que les technologies [ANT](#), [BLE](#) et 802.15.6 sont, de préférence, utilisées à un saut. Elles peuvent fonctionner à proximité du corps humain et ainsi permettre de relier les capteurs à un point de collecte ou à un autre nœud qui utilise la technologie [IEEE 802.15.4-2006](#) ou ultérieure. Ce nœud joue le rôle d'un collecteur ou de routeur qui transmet l'information reçue vers un point d'accès ou un centre de collecte distant. Pour le projet *CANet*, nous allons utiliser majoritairement la norme [IEEE 802.15.4](#) comme l'outil de base qui permet l'intégration d'autres technologies afin de satisfaire les contraintes du projet.

Dans cette partie, nous avons pu comprendre le rôle générique qui peut être joué par chaque technologie et avons décidé d'utiliser principalement la technologie [IEEE 802.15.4](#) dans le projet *CANet*, avec la possibilité de lui associer d'autres technologies selon les besoins de l'application. Dans la partie suivante, nous présenterons une étude complémentaire sur la qualité de service dans le réseau de capteurs afin d'identifier les verrous à lever dans ce domaine.

1.3 Qualité de service dans la littérature

De nombreuses applications dans les réseaux de capteurs nécessitent un niveau minimum de fiabilité dans la transmission de l'information. Pour satisfaire à ces exigences, de nombreux algorithmes de [QoS](#) sont cités dans la littérature.

Les algorithmes de QoS (cf. Figure 1.21) peuvent être divisés en deux sous-catégories : les algorithmes utilisés avec CSMA et ceux utilisés pour réserver des slots de temps (appelés [GTS](#) dans 802.15.4) pour les nœuds. La sous-classe CSMA est composée de 3 types d'algorithmes [P3, P6] :

- **différenciation par priorité** : la priorité est attribuée aux nœuds en fonction de l'importance de l'information détectée [66, 67],
- **différenciation par les paramètres d'accès** : les paramètres tels que [CW](#) (*Contention Window*), *backoff exponent* et [SIFS](#) (*Short InterFrame Space*) sont

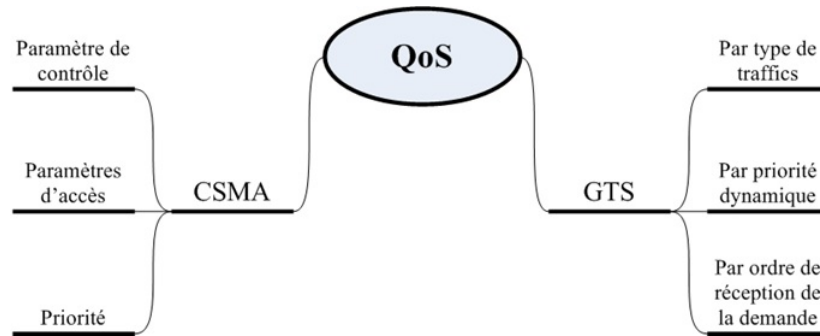


FIGURE 1.21: Classification des algorithmes de QoS dans 802.15.4

utilisés dans les méthodes d'accès avec des valeurs différentes pour les différents niveaux de priorité. La variation de ces valeurs accélère la transmission des paquets ayant une priorité élevée [68, 69],

- **différenciation par les paramètres de contrôle** : cette classe regroupe les algorithmes de **QoS** qui utilisent des paramètres tels que le nombre de sauts et la durée de vie d'un paquet pour contrôler le transfert des paquets dans le réseau. Les algorithmes utilisent ces paramètres pour différencier entre les trafics existants et attribuer des priorités [70].

La sous-classe **GTS** regroupe de nombreux algorithmes, qui sont proposés pour résoudre le problème de la réservation des slots dans 802.15.4. Cette sous-classe est divisée en 3 parties :

- **réservation selon l'ordre de réception de la demande** : le coordinateur réserve les slots aux nœuds demandeurs dans l'ordre de la réception des demandes. Si un nœud veut réserver un **GTS**, il envoie une demande au coordinateur, qui contient le nombre de slots désirés et le sens de l'échange (réception ou émission). Lorsque le coordinateur reçoit la requête, il compare le nombre de slots demandés avec le nombre de slots disponibles dans la période de la **CFP**. Si le nombre requis est inférieur ou égal au nombre disponible, le coordinateur attribue les slots nécessaires à ce nœud. Dans l'autre cas, le coordinateur rejette la demande,
- **réservation selon la priorité dynamique** : la réservation de **GTS** dépend de la priorité affectée à chaque nœud du réseau. Cette priorité assignée change dynamiquement en fonction de l'utilisation des derniers **GTS** réservés,
- **réservation selon le type du trafic** : dans cette troisième classe, l'attribution de **GTS** est adaptée pour le traitement des trafics temps réel. Dans la structure initiale de la supertrame 802.15.4, lorsqu'un nœud veut transmettre des données au cours de la **CFP**, il envoie une demande de **GTS** et attend la réponse dans le *beacon*. Si la demande est acceptée, le nœud ne transmet les paquets que dans la période réservée, ce qui rend la structure actuelle de la supertrame insuffisante pour soutenir la transmission des données en temps réel. Pour cette raison, il existe

des travaux qui proposent des algorithmes de réservation basés sur une extension du concept **GTS** qui est utilisé dans la norme 802.15.4 [71].

Nous venons de présenter rapidement différents concepts d'allocation de **GTS**, et nous les avons classifiés en trois classes. Par contre, nous avons identifié que les protocoles existants précédemment présentés ne prennent pas en considération la transmission des types de données de différentes catégories à travers un support physique unique.

Nous remarquons également que les protocoles proposés permettent aux nœuds demandeurs de **GTS** de réserver ces slots pendant une durée indéterminée, qui ne dépasse pas 14 supertrames ou dont la fin est liée à la libération des **GTS** qui se fait par une demande explicite.

La multitude des services offerts en *e-santé* impose d'avoir différentes classes de **QoS** qui varient selon les besoins de chaque application utilisée. Les études qui sont effectuées afin d'évaluer la performance et les besoins de **QoS** des différents services se composent de deux grands groupes : étude générale et étude spécifique pour des cas bien déterminés.

Parmi les études spécifiques, nous trouvons [72], [73] et [74] où les auteurs étudient des cas reliés à l'état d'urgence, où est discuté la mise en œuvre d'un système de santé. Dans [75], qui appartient aux études générales, les auteurs étudient la **QoS** dans le cas des nouvelles générations des architectures réseaux, en particulier dans le contexte de système **EPS** (*Evolved Packet System*) spécifiée par **3GPP** (*Third Generation Partnership Project*). Ils définissent un intervalle qui varie entre tolérant et intolérant pour le délai de transmission et pour la sensibilité à la perte de données puisque les exigences des services *e-santé* varient selon l'importance de l'information et la situation.

Après l'étude théorique que nous avons effectuée, nous avons pu proposer trois algorithmes d'ordonnancement des divers trafics générés par plusieurs applications [76]. Cette proposition initiale au début de nos travaux de thèse a été mise de côté car nous avons pu trouver une solution plus générale qui ne demande pas d'effectuer des modifications au niveau de la couche MAC, ce que nous nous sommes attachés à faire afin de rester le plus générique possible dans nos solutions proposées.

1.4 Conclusion

Les sociétés actuelles avancent à grand pas vers le "siècle des personnes âgées". La plupart des nations ont initié la préparation de lois pour l'adaptation de la société et la protection des personnes âgées. Les chercheurs et les industriels ont été très réactifs pour faire face à ce sujet par le lancement des projets de recherche et des applications ou produits qui visent l'amélioration de la qualité de la vie par le suivi et de la surveillance des personnes âgées.

Les organisations de standardisation ont participé également à ce mouvement par la création et l'amélioration des standards pour s'adapter aux besoins futurs des applications de surveillance.

Afin de mettre en lumière cette évolution et d'en comprendre les causes et les objectifs, nous avons présenté dans ce premier chapitre le domaine de l'*e-santé* d'une manière générale. Nous avons présenté les causes de l'apparition de cette nouvelle problématique et son importance dans le futur de la population mondiale et les exigences qui doivent être respectées. Nous avons ensuite présenté les technologies existantes et nous avons effectué une comparaison de ces dernières face à nos besoins afin de nous orienter finalement vers la norme [IEEE 802.15.4](#) comme technologie de base pour le projet *CANet* qui sera présenté dans le chapitre 2.

Notre orientation est donc de nous focaliser principalement sur la norme 802.15.4 comme support des liens radio autour de la canne, tout en conservant la possibilité d'ajouter une ou plusieurs autres technologies comme interfaces de communication distantes avec des sites éloignés, ou localement avec des implants ou des capteurs à la surface du corps humain. Finalement, nous avons présenté l'objectif de la thèse.

Dans le second chapitre, nous présenterons l'architecture réseau et protocolaire que nous avons proposée pour le projet *CANet* en détaillant nos choix. Nous étudierons alors plus finement la norme [IEEE 802.15.4](#) en proposant une solution pour la différenciation des trafics sans effectuer de modifications sur les spécifications définies dans le standard. Finalement nous terminerons cette partie par une étude théorique sur la transmission de la voix à travers la norme [IEEE 802.15.4](#).

Chapitre 2

Contribution technologique et modélisation architecturale

Plusieurs projets sont proposés dans le domaine de la *e-santé*, parmi eux, le projet *CANet* qui vise à surveiller une personne via des capteurs qui instrumentent une canne de marche communicante. Dans ce cadre s'inscrit le contexte général de notre thèse.

Dans le projet *CANet*, plusieurs types de données sont générées par des capteurs. Parmi ces informations, nous avons en particulier des données qui doivent être transmises dès leur réception comme les données d'alerte ou les informations sur l'état de la santé de l'utilisateur. Les informations générées par les capteurs de la canne vont passer, dans notre proposition d'architecture réseau, à travers une couche physique et une couche MAC afin d'être transmises à travers un lien sans fil vers un point d'accès fixe, lui-même relié à un point de collecte distant. Ceci pose un problème de respect des contraintes temporelles exigées par les trafics. Nous avons donc besoin d'un mécanisme protocolaire qui permette la gestion de divers trafics émanant des différents capteurs de la canne afin de les transmettre sur l'interface radio de cette dernière.

Afin de concevoir ce protocole, qui prend en considération la diversité des sources d'information reçue, nous avons décomposé l'objectif général de notre thèse en plusieurs sous-objectifs. Cette décomposition a pour effet, d'une part, de simplifier le processus de résolution du problème général, et d'autre part, de bien étudier et comprendre les détails de cette problématique. Nous présenterons, en premier lieu, le contexte et la problématique du projet *CANet*. Nous enchaînerons ensuite sur une proposition et une étude des capteurs qui peuvent être utilisés. Puis, nous proposerons une classification de ces capteurs par profils, pour aboutir à une virtualisation des caractéristiques et des types de capteurs. Cette classification générique peut s'adapter à tout capteur pouvant être ajouté dans le futur. Cette étude de profils ne peut pas être finalisée sans fixer alors la topologie globale qui sera ensuite utilisée dans la proposition d'une architecture protocolaire qui permet la différenciation des différentes données issues de ces profils de capteurs précédemment choisis. Cette architecture nécessite des paramètres de configuration qui seront fixés par une étude détaillée sur les paramètres **BO** et **SO** de la norme

IEEE 802.15.4. Finalement, nous terminerons ce second chapitre par la présentation d'une étude théorique de la transmission de la voix et une conclusion.

2.1 Contexte et problématique

Le projet *CANet* fédère plusieurs disciplines et compétences qui coopèrent entre elles afin de transformer une simple canne en un système embarqué qui permet la surveillance non intrusive tout en respectant la vie privée des personnes âgées en les maintenant non tributaires de tout besoin d'aide supplémentaire, grâce à un système de communication entre la canne et un centre de surveillance, local dans le cas d'une maison de retraite, ou distant dans le cas d'un maintien à domicile.

Le bilan médical optimal de la personne âgée porteuse de la canne nécessite que cette dernière soit équipée d'une multitude de capteurs, comme des capteurs audio, de température, de pression, d'accélération, de position...(cf. figure 2.1).

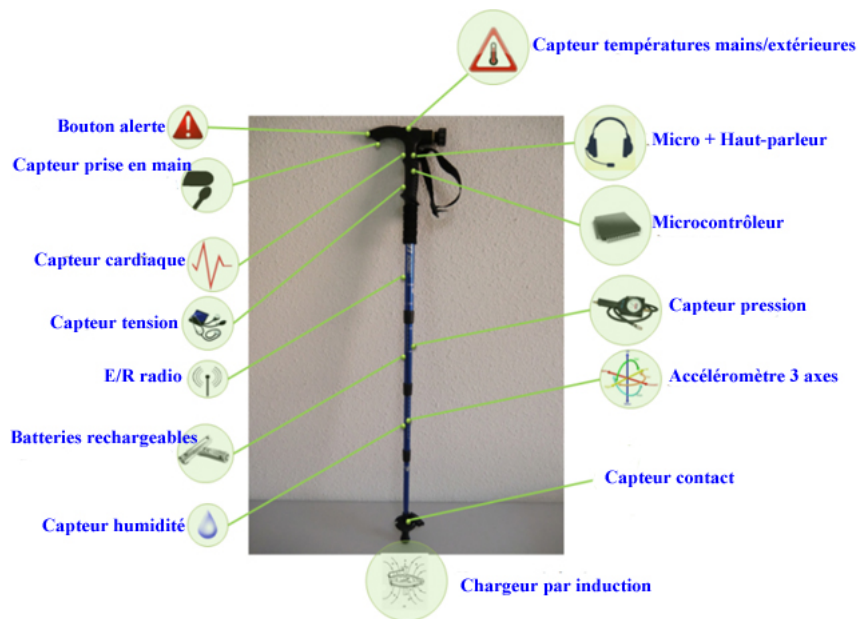


FIGURE 2.1: Exemple des capteurs inclus dans la canne

Les différents capteurs de la canne sont pilotés par un microcontrôleur embarqué. Ce dernier offre aussi à la canne un système de communication sans fil afin de permettre la transmission des informations collectées vers un centre de contrôle local ou distant. Le projet *CANet* prévoit parmi les capteurs d'intégrer un microphone et un haut-parleur qui seront utilisés pour lever le doute par communication vocale. Le type et le nombre de capteurs peuvent changer selon les pathologies des personnes âgées et le type d'information dont le personnel médical a besoin pour assurer une bonne qualité du suivi médical.

L'alimentation des composants électroniques de la canne s'effectue par des batteries rechargeables. Les batteries sont rechargées durant la nuit via un chargeur par induction

(les informations liées au niveau d'énergie dans les batteries seront aussi transmises vers le centre de contrôle pour gérer la situation dans le cas d'arrêt imminent du système, en particulier pour les personnes âgées sous contrôle continu).

Dans l'intention d'optimiser la consommation d'énergie et de ne pas générer de fausses alertes ou des informations erronées, la canne est équipée d'un capteur de prise en main permettant d'activer le système embarqué et d'informer le centre de collecte du début de l'usage de la canne ou de son arrêt.

Toutes ces informations représentent donc plusieurs types des données avec des caractéristiques différentes. Parmi ces informations, nous avons en particulier des données qu'il faut transmettre sans perdre de temps, comme des données très importantes dans le cas d'alertes ou des informations sur l'état de la santé de l'utilisateur, des données périodiques... Les informations générées par les capteurs vont passer à travers une couche physique et une couche MAC afin d'être transmises vers un point d'accès, lui-même relié à un point de collecte. Ceci pose un problème de respect des exigences temporelles. Nous avons donc besoin d'un mécanisme protocolaire qui permette la gestion des divers trafics émanant des différents capteurs de la canne pour pouvoir les transmettre sur l'interface radio de cette dernière. Pour cette raison, nos travaux de thèse sont principalement organisés autour de la conception d'une architecture réseau et protocolaire, et spécifiquement d'une méthode d'accès qui permettent la surveillance des personnes âgées à travers un réseau de capteurs embarqués dans une canne.

Plutôt que de tout modifier dans la couche 2, et par souci d'interopérabilité, l'architecture proposée ne doit pas imposer de changements majeurs au niveau de couche MAC mais elle doit utiliser les services offerts par cette dernière afin de réaliser les objectifs demandés. De plus, elle doit être adaptative pour s'adapter aux conditions environnementales de la personne. Par conséquent, l'architecture proposée doit offrir une diversité de services, parmi lesquels nous trouverons :

- la gestion de trafic,
- la gestion des priorités,
- la possibilité de transmettre des messages qui ne tolèrent pas un grand délai de latence comme pour la communication audio.

Dans la section suivante, nous étudierons un ensemble de capteurs qui peuvent être utilisés dans le projet *CANet*. Les capteurs choisis seront utilisés comme base et modèle pour la création des profils qui représentent d'une manière générale un ensemble de caractéristiques bien définies et génériques.

2.2 Profils de capteurs

Le nombre et les types de capteurs qui peuvent être utilisés dans le projet *CANet* dépendent de la pathologie de la personne et de la thérapeutique appliquée par les médecins. Pour avoir un suivi efficient, un ensemble d'informations nécessaires sont attendues. Ces informations imposent l'utilisation de catégories spécifiques de capteurs qui offrent des caractéristiques adaptées aux besoins de l'application. L'analyse approfondie de ces données doit offrir la possibilité de disposer d'un bilan exact de l'état de la santé de la personne âgée. Dans un premier temps, nous présenterons les capteurs susceptibles d'être utilisés dans le projet *CANet* et la problématique spécifique liée à leur utilisation. Nous étudierons ensuite leurs besoins respectifs en terme de trafics générés sur le réseau, pour en déduire des profils. Ceci nous ramènera, finalement, à classifier les différents capteurs.

2.2.1 Capteurs définis dans le projet CANet

Le traitement des données dans le projet *CANet* se fonde sur la corrélation entre les différentes informations médicales reçues. Chaque classe d'informations demande l'utilisation d'un type bien déterminé de capteur. La qualité des résultats d'analyse de l'état de santé de la personne âgée, utilisateur de la canne, dépend essentiellement du type et de la véracité des informations reçues. Par exemple, les premiers signes les plus connus d'une crise cardiaque sont [77] :

- **une douleur thoracique** : l'utilisateur de la canne doit avoir la possibilité d'appeler de l'aide. On a donc besoin d'un système d'alarme. Le projet *CANet* peut satisfaire ce besoin par l'utilisation d'un bouton d'alarme qui permet d'établir une communication vocale entre la personne âgée et le centre de contrôle,
- **des sueurs ou sudations** : dans ce cas, l'utilisation d'un capteur d'humidité de la main permet la détection du changement de niveau d'humidité de la main de l'utilisateur,
- **des nausées, vomissements et parfois indigestion** : ces signes demandent une communication vocale avec la personne âgée,
- **la peau qui devient froide et moite** : l'utilisation d'un capteur de température de la main permet au centre de collecte et contrôle de détecter ce signe,
- **la peur, l'anxiété et le déni** : dans ce cas, l'utilisation d'un système de communication vocale sera utile puisque la personne âgée a besoin d'avoir un aidant et un expert à ses côtés jusqu'à l'arrivée des secours.

Une suspicion de problème cardiaque peut être réalisée grâce à des capteurs spécifiques. Pour chaque pathologie, il existe des capteurs spécifiques qui permettent la détection de

leurs signes précurseurs. Ces capteurs génèrent des messages selon des caractéristiques bien définies afin de transmettre les informations collectées.

Le tableau 2.1 présente un ensemble de capteurs qui peuvent être utilisés dans le projet *CANet*. D'autres capteurs pourront aussi être utilisés. Ces capteurs ont des caractéristiques variées, qui impliquent des trafics réseau différents, ce qui rend leur différenciation complexe, ainsi que leur implémentation, pour le transport des données qu'ils génèrent. Cette complexité influence grandement les performances de l'application.



Capteur associé	Exemple du capteur	Rôle
Capteur TOR pour la détection de l'action de la canne sur le sol		Ce capteur permet de calculer la distance parcourue en fonction du nombre de pas, ce qui donne une idée sur l'activité effectuée par l'utilisateur de la canne (actimétrie).
Actionneur de mise en marche du système		Ce capteur permet à l'utilisateur saisissant sa canne de l'activer / éteindre
Capteur de température de la main		Ce capteur permet la mesure de la température de l'utilisateur à partir du contact établi entre le capteur et la peau de la main
Capteur de rythme cardiaque		Ce capteur est en mesure de surveiller le tissu vasculaire et d'envoyer des informations vers le centre de contrôle pour être traitées par l'équipe médicale
Capteur de température extérieure		Ce capteur permet la détection de la température de l'environnement autour de la personne âgée, ce qui doit être corrélé aux résultats des capteurs d'humidité et de température de la main
Microphone		Ces capteurs/actionneurs permettent d'établir une communication vocale avec la personne âgée, ce qui présente un support psychologique important dans les cas d'urgence
Haut-parleur		
Capteur de charge de batterie		Indique au centre de contrôle un risque d'arrêt imminent du système à cause de manque d'énergie dans la batterie, ce qui donne la possibilité à l'équipe de contrôle de prendre les précautions nécessaires
Capteur ou système de localisation		Le projet <i>CANet</i> propose l'utilisation de deux systèmes de localisation : Indoor (un algorithme de localisation [78] [79] [80]) et Outdoor (GPS). Cette information joue un rôle crucial dans les cas d'urgence, et permet une intervention rapide quelque soit le lieu de chute
Capteur d'humidité de la main		Ce capteur permet au centre de contrôle d'identifier les cas de sudation.
Capteur d'humidité extérieure		Les informations envoyées par ce capteur sont corrélées aux données reçues du capteur d'humidité de la main. Ainsi, ce capteur permet la détection des grandes variations d'humidité qui peuvent créer des problèmes de santé à la personne âgée
Accéléromètre 3D (et gyromètres)		Les accéléromètres permettent la détection d'une chute et donnent des informations sur : la rapidité de mouvement, la distance, la direction...
Bouton d'appel d'urgence		La personne âgée peut utiliser ce bouton si sa santé est en danger ou pour appeler au secours. Dès l'appui sur ce bouton, une communication vocale s'établit avec le centre de contrôle.

TABLE 2.1: Capteurs proposés pour le projet *CANet*

2.2.2 Critères de classification

La forte variation des caractéristiques et le grand nombre de capteurs qui peuvent être utilisés dans la même application doivent être vus comme une problématique face à un simple traitement spécifique à chaque type d'informations.

La proposition de critères généraux pour la classification des trafics selon des profils pouvant regrouper n'importe quel type de capteurs utilisés devient une nécessité, et devrait permettre la simplification du traitement qui sera effectuée pour chaque type de capteur.

A partir de la description des capteurs choisis dans le tableau 2.1, nous remarquons que les critères les plus pertinents et communs à tous sont : la périodicité, le débit nécessaire, la priorité et l'aspect temps réel.

2.2.2.1 Périodicité des données

La périodicité des données représente la durée du cycle de transmission pour chaque capteur. Cette durée varie selon le type d'information et la période utile qui permet la détection des informations significatives. Par exemple, le changement de la température du corps humain ne se fait pas chaque seconde ; par conséquent, la nécessité de connaître la température chaque seconde n'est pas obligatoire. Par contre, dans le cas de la cardiopathie, les informations sur les performances du cœur humain sont importantes. Le suivi permanent et continu est obligatoire. Il n'est pas acceptable de laisser passer une minute sans avoir reçu les renseignements envoyés par le capteur responsable de la collecte des données de cet organe vital. La perte ou le retard dans la réception des messages envoyés, dans ce cas, représente une interruption dangereuse dans la procédure de surveillance et de contrôle. À partir de cet exemple, nous déduisons que chaque capteur doit avoir un traitement spécifique qui dépend de la périodicité de transmission des informations collectées. Ainsi, nous constatons l'existence des différentes catégories de périodicité. Généralement, nous allons différencier quatre familles qui peuvent représenter tous les capteurs de la canne :

- des capteurs associés à une **pseudo périodicité** : dans cette catégorie, nous trouvons les trafics inégaux et souvent non prédictibles qui obéissent à une période mais pour des cycles irréguliers. Ces trafics ne sont pas toujours présents, comme :
 - les informations d'urgence,
 - les données temps réel comme pour la communication vocale,
- des capteurs associés à une **périodicité faible** : les capteurs de cette catégorie génèrent des informations avec une fréquence élevée. La durée entre deux transmissions successives est très faible. Dans cette famille, nous trouvons, par exemple, le capteur de rythme cardiaque,

- des capteurs associés à une **périodicité moyenne** : dans cette catégorie, la période entre deux transmissions successives est de l'ordre de quelques minutes. Dans cette famille, nous trouverons par exemple le capteur [TOR](#),
- des capteurs associés à une **longue périodicité** : cette catégorie regroupe les capteurs qui génèrent des informations avec une fréquence très faible. La durée entre deux transmissions successives dépasse celle de la famille de périodicité moyenne. Les capteurs que nous pouvons retrouver dans cette catégorie sont dédiés par exemple de la mesure à la température ou de l'humidité.

Il apparaît clairement que la limite entre les quatre catégories n'est pas évidente, ce qui entraîne une situation équivoque lors du classement des capteurs. Pour éviter cette problématique, nous avons défini **plusieurs paramètres** ainsi que **plusieurs règles** qui permettent de simplifier et clarifier la tâche de classement des capteurs.

Définition 2.1 : le paramètre *Seuil Haut* ([SH](#)) représente un seuil pour la durée maximale de chaque cycle de transmission utilisé par les capteurs. La durée maximale de [SH](#) est égale à 10 min, par défaut.

Définition 2.2 : le paramètre *Seuil Bas* ([SB](#)) représente un seuil pour la durée minimale de chaque cycle de transmission utilisé par les capteurs. La durée minimale de [SB](#) est égale à 1 min, par défaut.

Ces règles nous permettent d'identifier la catégorie d'appartenance d'un capteur :

Règle 2.1 : si la périodicité utilisée par le capteur pour transmettre les informations est inférieure à [SH](#) et supérieure à [SB](#), alors le capteur appartient à la catégorie **périodicité moyenne**. Si la périodicité utilisée est supérieure à [SH](#), alors le capteur appartient à la catégorie **longue périodicité**. Si la périodicité utilisée par le capteur pour transmettre les informations est inférieure à [SB](#), alors le capteur appartient à la catégorie **périodicité faible**.

Règle 2.2 : si la périodicité utilisée par le capteur n'est pas régulière ou si elle est régulière uniquement durant un intervalle de temps, c'est-à-dire non continue, alors ce capteur appartient à la catégorie **pseudo-périodicité**.

2.2.2.2 Débit nécessaire

Nous nous intéressons au débit utile nécessaire pour la transmission des informations collectées par chaque capteur. Dans les architectures classiques de réseaux de capteurs, les informations transmises sont souvent homogènes (détection d'incendie, etc.). Cette propriété ne s'applique pas dans le cas des applications e-santé puisque nous n'avons pas une homogénéité des informations collectées par les capteurs. Cette différence de trafic influence fortement la durée de transmission donc la période d'occupation du canal

par le capteur. Connaître la classification des capteurs selon la durée nécessaire pour la transmission, est donc une aide pour prendre des décisions sur la priorité pour accéder au canal.

Dans le projet *CANet*, nous avons classé les trafics générés par les capteurs selon trois catégories de débits :

- **faible** : les données envoyées par les capteurs de cette catégorie ne dépassent pas quelques octets par seconde. Ce trafic ne demande pas une longue période de transmission. Par conséquent, il n'est pas susceptible de créer un problème au niveau de réseau. Les capteurs de cette catégorie envoient par exemple des informations liées à la température, au nombre d'appuis sur le sol...
- **moyenne** : cette catégorie concerne des données plus volumineuses. Généralement, elle est liée aux informations qui offrent une représentation 2D ou 3D comme les données de localisation intérieur, de [GPS](#)...
- **grand** : les trafics temps réels sont le plus volumineux parmi tous les trafics présentés dans les autres catégories car, généralement, ces trafics contiennent des données d'un message vocal et nécessitent une grande bande passante. Les capteurs de cette catégorie offrent un trafic nécessaire qui peut occuper toute la bande passante pour une durée variable non déterminée, ce qui peut créer un problème de famine pour les autres. Ce type de trafics nécessite un traitement spécifique qui dépend de son volume et importance. Les échanges de type audio sont un exemple typique.

La différence entre les trois familles du trafic est très générale et assez adaptable, ce qui rend le choix de la famille tributaire des règles fixées par chaque utilisateur. Afin d'unifier le choix de la catégorie, nous avons défini un paramètre et une règle de classification :

Définition 2.3 :

- Le paramètre **Trafic Moyen Bas** ([TMB](#)) représente un seuil pour les trafics qui appartiennent à la catégorie du trafic nécessaire faible (typiquement [TMB](#) = 40 bits/s).
- Le paramètre **Trafic Moyen Haut** ([TMH](#)) représente un seuil pour les trafics qui appartiennent à la catégorie du trafic nécessaire moyen (nous avons typiquement [TMB](#) < [TMH](#) < 10 kbit/s).

Règles 2.4 :

- Si le trafic nécessaire est inférieur à [TMB](#), alors le capteur appartient à la catégorie du trafic nécessaire faible.

- Si le trafic nécessaire est entre **TMB** et **TMH**, alors le capteur appartient à la catégorie du trafic nécessaire moyen.
- Si le trafic nécessaire est supérieur à **TMH**, alors le capteur appartient à la catégorie du trafic nécessaire grand.

Les règles définies doivent satisfaire la condition suivante : $0 < \text{TMH} < \text{TMB}$.

2.2.2.3 Priorités

Dans la section 2.2.1, nous avons cité les symptômes d'une crise cardiaque. Parmi les signes vitaux précurseurs, nous avons identifié tout particulièrement les variations du rythme cardiaque. Nous avons également répertorié des signes qui nécessitent une communication vocale ou un appel à l'aide. Dans ce cas, nous pouvons considérer que la personne demande de l'aide grâce à un bouton d'appel d'urgence, couplé simultanément à une transmission de son rythme cardiaque. Ces deux capteurs transmettent donc des données avec un trafic et une périodicité différente. La canne peut différencier les deux flux de données indépendants et non simultanés grâce aux deux critères précédemment présentés. Mais, elle ne peut pas décider ce qu'il advient lorsqu'elle reçoit les deux flux en même temps. Par conséquent, la question qui se pose dans ce cas là est de déterminer quel est le trafic le plus prioritaire.

Pour l'être humain, la communication vocale qui sera établie grâce à l'appel à l'aide est généralement considérée comme plus prioritaire, par rapport aux informations du capteurs de rythme cardiaque. Cependant, le système embarqué dans la canne ne peut pas prendre cette décision sans avoir un indicateur qui l'aide à différencier les informations prioritaires des autres types de flux existants. A partir de cette analyse, nous avons décidé d'ajouter un nouveau critère de classification qui représente un indicateur de niveau de priorité des informations générées par la canne.

Dans la présentation des capteurs (cf. tableau 2.1), nous remarquons que les capteurs génèrent trois types de données :

- données de type **temps réel** : ces données induisent des exigences au niveau de la latence, du débit, de la gigue et du nombre de paquets perdus,
- **les données d'alerte** : ce sont des trames qui contiennent des informations d'urgence. Ces trames sont créées par les capteurs lors de la détection d'une variation anormale du signe vital,
- **des données tolérantes** : ces données représentent les informations qui n'imposent pas des exigences temporelles et de **QoS**.

Donc, trois niveaux de priorité doivent être définis :

- **priorité faible** (**LP** : *Low Priority*): cette catégorie contient les données tolérantes,
- **priorité forte** (**HP** : *High Priority*): cette catégorie contient les données temps réel,
- **priorité très forte** (**VHP** : *Very High Priority*): cette catégorie contient les données d'alerte.

Ces trois niveaux de priorité nous permettent de classer les capteurs selon leur type de données émises.

2.2.3 Classification des capteurs

Dans les deux premières sections de ce chapitre, nous avons présenté les capteurs qui peuvent être utilisés dans le projet *CANet* et les critères essentiels pour leur classification. Ces derniers seront utiles pour identifier les profils associés aux capteurs, tout en simplifiant le traitement protocolaire dédié à chaque type d'information générée par ou à destination de la canne. L'étape de classification des capteurs est en fait la troisième phase après le choix des capteurs et des différents critères. Les différents capteurs seront classifiés en un ensemble de profils en fonction des critères définis ci-dessous. A partir de ce classement, nous identifierons les différents profils existants dans le projet *CANet*.

L'étude des capteurs, précédemment présentée, a révélé l'importance de prendre en compte l'état critique et l'alerte sous forme de profils généraux. L'état critique représente le passage vers une situation de contrôle extrême après avoir détecté une variation anormale dans les données détectées par les capteurs. L'état d'alerte représente la demande de l'utilisateur d'établir une communication vocale pour demander de l'aide.

Ces profils seront utilisés par tous les capteurs lors de l'existence d'un état critique, lors de la détection d'une anomalie ou lors de l'envoi d'une alerte, qui indiquent l'existence d'un problème médical. Cette généralisation rend ainsi le traitement de ce type d'information homogène. Pour cette raison, nous avons ajouté deux profils spécifiques que nous estimons capitaux dans le cas des applications de surveillance et de contrôle. Le premier profil ajouté est associé à la trame d'alerte. Cette trame est caractérisée par une quantité de données très réduite, donc un débit généré faible, mais une priorité très forte. Elle doit être la plus prioritaire dans le réseau. Afin d'identifier les capteurs qui ont la possibilité d'envoyer des trames d'alertes, nous avons ajouté un critère nommé "**alerte**" aux critères de classifications. Tous les capteurs qui ont la possibilité de générer une alerte peuvent utiliser les caractéristiques associées au profil "**trame d'alerte**" lors de l'émission de cette dernière. De plus, nous avons ajouté le profil "**état critique**". Ce profil est caractérisé par une diminution de la période d'acquisition et d'émission des données du capteur, ce qui rend le suivi de la personne âgée plus précis et plus réactif. Tous les capteurs susceptibles d'être capables de fournir la moindre information pouvant

sauver la vie de l'utilisateur de la canne, sont donc associés à ce profil spécifique que nous avons numéroté 10.

Le tableau 2.2 présente les critères des informations générées par les capteurs et les profils associés à ces derniers. À partir de ce tableau, nous constatons qu'il existe donc 10 profils différents, dont 8 représentent les différentes caractéristiques des capteurs, auxquels nous adjoignons deux profils supplémentaires représentant les caractéristiques spécifiques de "**l'état critique**" et du bouton "**d'appel d'urgence**".

Capteur	Périodicité			Débit nécessaire			Priorité			Alerte	Profils	
	Pseudo	Faible	Moyenne	Longue	Faible	Moyen	Grand	LP	HP			VHP
Capteur de prise en main	✓				✓			✓			1	
Capteur de température de la main				✓	✓			✓		✓	2/9/10	
Capteur de température extérieure				✓	✓			✓		✓	2/9/10	
Capteur de la charge de batterie				✓	✓			✓		✓	2/9	
Capteur d'humidité du corps humain				✓	✓			✓		✓	2/9/10	
Capteur d'humidité extérieure				✓	✓			✓		✓	2/9/10	
Capteur TOR pour la détection de l'action de la canne sur le sol			✓		✓			✓			3/10	
Microphone											4	
Haut-parleurs	✓						✓		✓			
Un ou plusieurs accéléromètres		✓				✓			✓		5/10	
Bouton d'appel d'urgence	✓								✓		6	
Système de localisation			✓			✓			✓		7/9/10	
		✓				✓			✓			
Capteur de rythme cardiaque		✓				✓		✓		✓	8/9/10	
Trame d'alerte	✓					✓					9	
Etat critique		Les caractéristiques de ce profil seront définies par la suite										10

TABLE 2.2: Classification des capteurs en profils

Chaque profil représente un ensemble de caractéristiques communes entre les capteurs qui lui sont associés. Nous avons rassemblé chaque ensemble d'informations (périodicité, débit, priorité) sous un profil pour pouvoir simplifier la représentation des caractéristiques et regrouper les capteurs qui se verront appliquer un même traitement dans un seul et même ensemble (cf. tableau 2.2).

Dans le cas où un capteur appartient à plusieurs profils, le profil de base est écrit en gras en première position. Nous trouvons ensuite les deux profils secondaires. Par exemple, si un capteur appartient au profil 2/8/10, nous pouvons déduire que ce capteur est habituellement caractérisé par les mêmes spécificités que celles du profil 2 (périodicité, débit, priorité) ; il peut également envoyer des trames d'alertes (profil 8). Enfin, il peut modifier ponctuellement ses caractéristiques en utilisant celles qui caractérisent le profil 10 lorsqu'un état critique est déclenché (l'état critique se déclenche lorsqu'un capteur émet un message d'alerte).

La norme IEEE 802.15.4 définit deux techniques d'accès au canal différentes : CSMA/CA et TDMA. La technique CSMA/CA est utilisée dans la période CAP. Cette technique n'assure pas une bonne qualité de service et présente le risque qu'un nœud monopolise le canal si l'un des capteurs émet sur le médium sans avoir l'intention de céder la place aux autres capteurs pour qu'ils transmettent leurs propres informations. Ce dernier point est potentiellement occurent dans le cas des applications e-santé, essentiellement dans le cas d'urgence. La technique TDMA est associée à la période CFP. La norme indique la possibilité d'attribuer des slots pour les capteurs demandeurs, ce qui représente un avantage important pour eux. Ainsi, la période CFP permet d'offrir une bonne QoS qui est une demande de contrainte forte pour les informations critiques.

La présence des deux périodes d'accès au médium dans la norme IEEE 802.15.4 répond ainsi aux besoins des différents profils que nous avons définis. Nous associons à chaque profil de capteur la période d'accès la plus adéquate.

Dans le tableau 2.3, nous pouvons remarquer que certains profils (6 et 9) utilisent les deux périodes CAP et CFP pour transmettre leurs informations. Face à l'importance de certaines informations et à la nécessité de leur émission au plus vite, nous avons décidé de pouvoir les transmettre dans les 2 périodes, et ainsi utiliser celle qui est la première à arriver au cours du temps. De plus, dans le cas de ces profils (6 et 9), les messages doivent absolument arriver à leur destination, nous avons choisi de dupliquer les informations et les envoyer dans les deux périodes CAP et CFP afin d'augmenter les chances qu'au moins un message arrive à la destination. Dans le cas de l'état critique, les profils conservent les mêmes périodes de transmission avec l'augmentation du nombre de messages d'information générés, ce qui implique la diminution de la périodicité de génération des messages.

Cette composition de profils des capteurs permettra à l'application de profiter au mieux des technologies protocolaires développées et définies dans la norme IEEE 802.15.4. Notre objectif est la satisfaction des différentes exigences des profils sans l'obligation d'effectuer des modifications majeures au niveau de la norme.

Capteur		Profils	Période
Capteur de prise en main		1	CAP
Capteur de température de la main		2/9/10	
Capteur de température extérieure		2/9/10	
Capteur de la charge de batterie		2/9	
Capteur d'humidité du corps humain		2/9/10	
Capteur d'humidité extérieure		2/9/10	
Capteur TOR pour la détection de l'action de la canne sur le sol		3/10	
Capteur de rythme cardiaque		8/9/10	
Microphone		4	CFP
Haut-parleurs			
Accéléromètres 1, 2 ou 3D			
Bouton d'appel d'urgence		6	CAP et CFP
Système de localisation	Extérieur	7/9/10	CFP
	Intérieur		
Trame d'alerte		9	CAP et CFP
Etat critique		10	–

TABLE 2.3: Périodes de transmission associées à chaque profil

Après cette étude détaillée des capteurs sélectionnés pour le projet *CANet*, nous les avons classifiés en différents profils. Cette étude reste, en l'état, incomplète car nous n'avons pas encore défini les paramètres les plus adaptés pour respecter les exigences de chaque profil. Ces paramètres dépendent également de l'architecture topologique du réseau qui sera proposée. Pour cette raison, la finalisation de cette étude des profils nécessite la présentation de l'architecture de communication globale proposée. Dans la section suivante, nous présenterons l'architecture globale que nous proposons.

2.3 Topologie globale proposée

Les applications de suivi et de surveillance dans le domaine de l'*e-santé* imposent l'utilisation de topologies de réseau souvent basées sur un seul niveau, avec comme entité maîtresse, un smartphone, ce qui est très simple mais présente de nombreuses lacunes, en particulier pour les personnes âgées qui n'en utilisent pas. D'autres topologies plus évoluées comportent parfois plusieurs niveaux. Cette complexité dans la conception doit être associée aux variantes de fonctionnalités exigées et à l'importance de l'information envoyée par ces applications.

2.3.1 Problématique spécifique

Suite aux études bibliographiques présentées dans le début du manuscrit, nous nous orientons tout naturellement vers une topologie basée sur l'utilisation de la norme [IEEE 802.15.4](#), avec des nœuds fixes dans l'habitat.

Le rôle des cannes de marche et des nœuds fixes, que nous qualifierons de points d'accès (PA), entraîne alors tout naturellement une problématique intéressante à relever puisque ces PA peuvent être : RFD, FFD ou éventuellement ni l'un ni l'autre.

Nous identifions également alors plusieurs types de liens possibles :

- entre la canne et les points d'accès,
- entre les points d'accès,
- entre les points d'accès et un serveur de collecte de données (distant ou local à l'habitat suivant qu'il s'agisse d'une surveillance à domicile ou dans un établissement spécialisé type Établissement d'hébergement pour personnes âgées dépendantes (EHPAD)),
- entre le serveur de collecte de données et le centre de traitement de données (lui aussi local ou distant suivant les cas),
- et éventuellement entre les différents capteurs de la canne ou ceux déportés directement sur la personne pour des raisons liées à la nature même des informations et des possibilités offertes par les capteurs actuels.

Chaque liaison exige des contraintes au niveau du débit, du type de trafic, de la taille de la zone de couverture, de la latence...

Dans la section suivante, nous présenterons la topologie proposée et nous justifierons nos choix.

2.3.2 Topologie proposée

Nous proposons une topologie à plusieurs niveaux afin de s'affranchir des problèmes de portée, de débit et de consommation énergétique. La communication entre les capteurs de la canne et le centre de collecte passe donc par plusieurs liaisons. Chaque liaison doit vérifier les caractéristiques requises pour respecter la qualité des communications désirées.

Cette topologie peut être composée de trois, quatre ou cinq niveaux :

- **Niveau 1** : liens entre la canne et les capteurs du corps humain (capteurs embarqués sur la personne). Ce niveau peut être omis.
- **Niveau 2** : liens directs entre cannes dans le cas d'un établissement type EPHAD où cohabitent plusieurs personnes âgées. Ce niveau peut être omis car les cannes ne sont pas faites initialement pour router les informations des autres cannes. Se pose également le problème de la confidentialité et la sécurité des informations des utilisateurs des cannes qui devrait être renforcée, par un chiffrement adapté, par

exemple. Malheureusement, ce type de liaison sécurisée et de relais entre cannes pourrait entraîner une utilisation plus importante de l'énergie de la canne. C'est pour cette raison que ce type de liaison ne sera pas considéré,

- **Niveau 3** : liens entre canne et PA. Dans ce cas, nous avons deux solutions potentielles si nous utilisons la technologie IEEE 802.15.4 pour ces liaisons :
 - chaque PA joue le rôle de coordinateur (FFD) et chaque canne est un équipement terminal,
 - chaque canne joue le rôle de coordinateur et chaque PA est un terminal.
- **Niveau 4** : liens entre PA,
- **Niveau 5** : liens entre PA et centre de collecte.

Les différents niveaux seront détaillés par la suite. Pour chaque niveau, nous expliciterons la solution retenue et argumenterons nos choix.

2.3.2.1 Niveau 1 : liens entre la canne et les capteurs du corps humain

La canne joue un rôle majeur dans le projet *CANet* puisqu'elle est le premier intermédiaire entre les capteurs et le centre de collecte d'informations. À ce niveau, la canne relaie les informations envoyées par les capteurs vers un ou plusieurs PA fixes de l'habitat. Mais, elle conserve le droit d'effectuer des prétraitements sur les informations avant la transmission, en particulier pour limiter les données émises. La communication entre le système embarqué dans la canne et ses capteurs associés peut être établie par une interface de communication sans fil ou par des liens filaires directs lorsque les capteurs sont répartis sur la canne elle-même. Pour les capteurs déportés sur le corps humain, nous proposons que la solution retenue se base sur la technologie ANT (voir 1.2.2.4) [81] (nous le justifierons par la suite), associée à une topologie étoile. Le centre de cette étoile est la canne, les capteurs sur le corps sont aux extrémités de chaque branche de l'étoile, comme nous le montre la figure suivante.

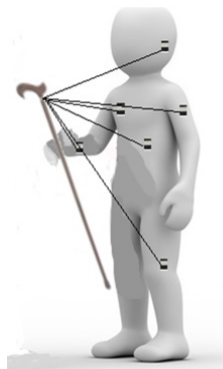


FIGURE 2.2: Relation entre les capteurs corporels et la canne

Cette topologie a le mérite d'être simple, évite les problèmes de synchronisation (qui auraient pu être rencontrés si nous avions attribué le rôle de maître aux capteurs) et limite la consommation d'énergie grâce à l'utilisation de la technologie ANT [81]. De plus, de nombreux capteurs médicaux ANT sont disponibles, même si aujourd'hui, il semble que la technologie BLE prenne le dessus d'un point de vue commercial, et non pour des raisons technologiques. Des topologies plus complexes de type maillées seraient envisageables pour réduire les problèmes de portée autour du corps humain, et pourraient être étudiées dans les perspectives de nos travaux. Notre thèse s'étant initialement attachée à proposer une architecture protocolaire où seuls les capteurs de canne étaient utilisés, nous n'avons pas plus creusé cette variante imposée par la présence de capteurs nécessairement sur le corps humain. Nos travaux sur ANT pourraient également trouver un prolongement par une comparaison avec la technologie BLE en perspective de notre thèse, mais aussi avec le nouveau standard IEEE 802.15.6 [82].

2.3.2.2 Niveau 2 : liens directs entre cannes

Pour ce niveau optionnel de la topologie globale proposée, nous avons étudié la possibilité d'avoir des communications directes entre les cannes, en particulier pour les messages d'alerte.

L'intérêt de ce type de communication réside dans la transmission des messages urgents lorsque la canne émettrice ne peut pas établir un lien avec un PA. La transmission des données d'analyse et de suivi n'est alors pas possible. Il pourrait être intéressant d'étudier plus finement ce type de liens directs, même si des problèmes de consommation énergétique des cannes surviendraient. Pour ce genre de raisons, il n'est pas souhaitable d'avoir des échanges d'informations classiques entre les cannes. La solution retenue est de placer suffisamment de PA pour assurer au moins un lien toujours possible à chaque canne.

2.3.2.3 Niveau 3 : liens entre cannes et PA

Pour ce niveau topologique, le choix paraît évident puisque le point d'accès n'a pas de contraintes énergétiques et n'est pas mobile. Ces caractéristiques rendent le PA l'entité la plus adaptée pour jouer le rôle de maître. Ce choix stratégique nous permet d'éviter tous les problèmes liés à la consommation d'énergie, la synchronisation, la gestion du réseau.

La topologie la plus adaptée pour ce niveau est la topologie étoile puisque toutes les cannes ont les mêmes caractéristiques et jouent le même rôle dans le réseau. Notre choix se porte bien sûr sur l'utilisation de la norme IEEE 802.15.4 pour ce type de liens, nous le justifierons par la suite. L'étoile peut avoir un seul ou plusieurs esclaves dans le cas de présence de plusieurs personnes dans une même pièce ou zone de portée du PA. Une canne ne peut s'associer qu'à un seul PA. Aucune relation directe ne peut être

établie entre les capteurs et les **PA** de technologies différentes, seules les cannes peuvent transmettre les informations des capteurs vers les **PA**. C'est donc par ce lien unique que toutes les informations issues ou destinées à la canne convergeront. Ce lien constitue donc un goulot d'étranglement potentiel et devra être bien dimensionné et finement géré.

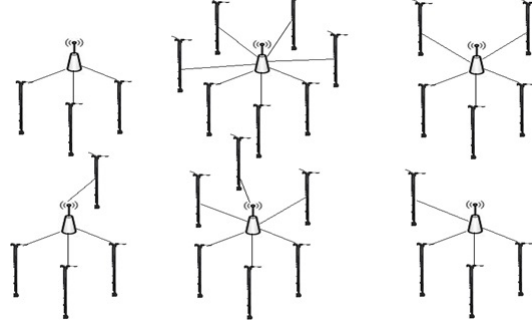


FIGURE 2.3: Modélisation de la topologie canne-PA

2.3.2.4 Niveau 4 : liens entre PA

Dans ce niveau, les **PA** sont responsables de la réception, le relayage et le routage des messages envoyés par les cannes. Nous n'avons pas ici de problème d'énergie, ni de problème de puissance de traitement de données. L'existence de plusieurs **PA** est dictée par la taille importante des zones de déambulation des personnes âgées, en particulier en milieu médical.

Trois topologies sont possibles pour établir une communication entre les **PA** : maillée, étoile et arbre. La topologie la plus adaptée et la plus souple est la topologie maillée puisque tous les **PA** ont le même rôle et sont de même type. Nous envisageons de nous baser sur la technologie **IEEE 802.11** pour ce niveau 4, comme nous le justifierons par la suite. Les nœuds peuvent utiliser un routage dynamique, ce qui permet d'éviter les routes saturées et les engorgements. Ce travail ne faisant pas partie directement de notre sujet, nous ne l'avons pas traité, mais avons travaillé en parallèle dans le projet ACOCASP [83] avec une autre doctorante de l'équipe, dont c'était le sujet principal [84, 85]. Des travaux complémentaires sur un réseau de capteurs comportementaux, menés par une autre doctorante de l'équipe peuvent également fournir des pistes de réflexions sur cette problématique [86].

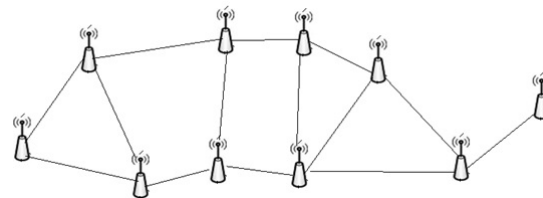


FIGURE 2.4: Topologie maillée des PA

2.3.2.5 Niveau 5 : lien avec un centre de collecte

Dans ce niveau ultime, nous avons identifié plusieurs solutions possibles selon le lieu d'installation du serveur de collecte d'informations. Si le serveur est local, nous pouvons utiliser simplement un réseau Ethernet, un réseau Wifi ou CPL (Courants Porteurs en Ligne). Si le serveur est distant, nous pouvons dans ce cas utiliser un réseau Internet, 3/4G ou même des liens satellites pour des zones où l'infrastructure Internet et téléphonique n'est pas bien implantée.

Dans le cas du serveur distant, il faut se baser sur des passerelles qui nous permettent de sortir du réseau local vers une destination distante éloignée. Cette passerelle doit être capable d'utiliser l'une ou l'autre des différentes technologies énoncées ci-dessus. Elle pourrait avantageusement être utilisée pour assurer également le suivi des personnes âgées en extérieur mais ceci sort du cadre de notre thèse.

2.3.3 Vue globale de la topologie choisie

La topologie globale proposée contient donc quatre niveaux différents. Chaque niveau assure la présence d'un lien entre deux éléments de niveaux différents (voir figure 2.5). Cette collaboration offre la capacité de transmettre les informations envoyées par les capteurs entre les différents niveaux de la topologie.

La figure 2.5 représente les différentes relations entre les éléments de la topologie. En résumé, la topologie proposée contient deux topologies étoiles (entre la canne et les capteurs ; et entre la canne et le PA) et une topologie maillée (entre les PA).

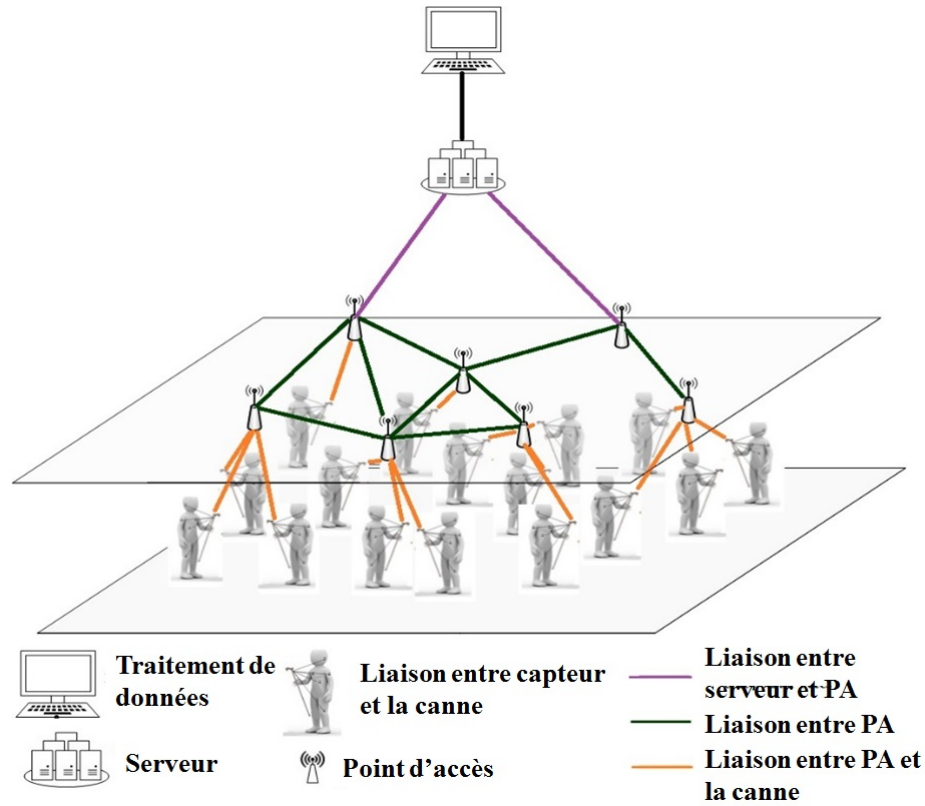


FIGURE 2.5: Topologie globale retenue

2.3.4 Solutions technologiques proposées

Dans la section précédente, nous avons présenté les topologies qui seront utilisées entre les différents niveaux. La définition de la topologie seule ne suffit pas pour atteindre un fonctionnement qui respecte la description des besoins de chaque niveau. Nous présenterons donc maintenant la solution technologique choisie pour chaque niveau.

Pour le premier niveau, l'utilisation de capteurs oriente vers des systèmes de communication à faible consommation d'énergie. Dans le premier chapitre, précisément dans la section 1.2, nous avons comparé les technologies qui peuvent être utilisées dans le projet *CANet* et nous avons conclu que les technologies [ANT](#) et [BLE](#) sont sur le même niveau technologique. Nous avons préféré [ANT](#) au début de la thèse face à la disponibilité de nombreux capteurs dédiés au domaine de la santé. Il semble qu'en 2015, BLE prenne un essor plus grand avec l'adoption de ce standard dans de nombreux smartphones et tablettes.

Le second niveau de la topologie, liens directs entre les cannes, ne sera pas étudié dans le cadre de cette thèse.

Pour le troisième niveau de la topologie, nous proposons d'utiliser la technologie [IEEE 802.15.4](#). Cette technologie nous permet d'avoir des périodes de transmission avec la technique [CSMA/CA](#) et des périodes avec la technique [TDMA \(GTS\)](#), ce qui va satisfaire les besoins de tout type d'informations générées par les capteurs. C'est sur ce niveau

utilisant IEEE 802.15.4 que se concentrent principalement nos contributions, avec en particulier une couche différenciation que nous proposerons en section 2.4. La canne, dans ce mode, jouera également le rôle de passerelle. Elle utilise donc les empilements protocolaires de deux technologies afin d'adapter les messages reçus des capteurs par la technologie ANT au format des messages utilisés par la technologie IEEE 802.15.4.

Pour le quatrième niveau, les liens entre les PA seront établis par la technologie IEEE 802.11. Cette technologie nous offre un lien WiFi massivement disponible, ce qui simplifie l'installation et offre un coût de déploiement réduit. La technologie IEEE 802.11 propose plusieurs standards qui utilisent des topologies et définissent des caractéristiques différentes. Plusieurs solutions peuvent être utilisées pour créer la topologie maillée, comme IEEE 802.11s [87] pour des réseaux à taille réduite avec une notion de diffusion entre PA, sans pour autant utiliser la fonctionnalité de PA sur l'interface IEEE 802.11. D'autres solutions basées sur un routage sont envisageables, comme OLSR [88] par exemple, à condition de pouvoir utiliser l'interface physique en mode adhoc. Au niveau physique et MAC, l'utilisation de IEEE 802.11n [89] semble aujourd'hui la bonne piste de solution pour obtenir des débits importants.

En résumé, cet équipement fixe va jouer trois rôles en même temps : point d'accès, point de maillage et coordinateur IEEE 802.15.4. Ceci signifie que nous devons ajouter le rôle de coordinateur de réseau à la fonction MAP (*Mesh Access Point*). Pour ces raisons, nous l'avons nommé CMAP (*Coordinator Mesh Access Point*). Le CMAP joue bien le rôle de passerelle entre les technologies IEEE 802.15.4 et 802.11s.

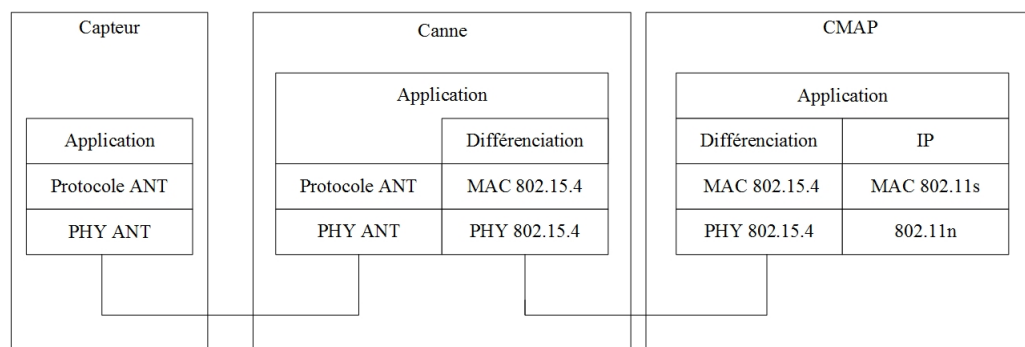


FIGURE 2.6: Relation entre les différentes technologies

La figure 2.6 représente les relations entre les différentes technologies établies dans chaque élément de la topologie globale. Les capteurs implémentent seulement les couches de la technologie ANT. Par contre, les cannes doivent implémenter les couches protocolaires ANT et IEEE 802.15.4. Ces deux empilements doivent être capables de recevoir et de transmettre les messages avec la couche application de la canne, ce qui lui donne la possibilité d'effectuer des prétraitements sur les informations reçus.

La communication entre la canne et le CMAP s'effectue à travers IEEE 802.15.4. Le CMAP implémente les deux normes IEEE 802.15.4 et IEEE 802.11. Nous sommes donc en présence d'un pont, si aucune modification applicative ni de prétraitement ne sont réalisées au niveau du CMAP.

Sur le plan fréquentiel, nous utilisons des technologies qui travaillent dans la même bande de fréquence [ISM](#) à 2.4 GHz, ce qui pourrait créer des problèmes de coexistence. Plusieurs recherches ont été effectuées pour trouver une solution qui permette la coexistence entre [IEEE 802.15.4](#) et [IEEE 802.11](#). Dans [90] les auteurs proposent une solution qui se base sur le [CCA](#) (*Clear Channel Assessment*), ce concept est appelé [CACCA](#) (*Coexistence Aware CCA*). Cette solution permet l'utilisation de la même fréquence par deux technologies différentes. Dans [91] et [92], les auteurs ont évalué les performances du réseau dans le cas du partage de la bande de fréquence 2.4 GHz entre [IEEE 802.15.4](#) et [IEEE 802.11 b/g](#) à travers un modèle et un testbed. Dans cette étude, les auteurs ont montré l'influence de l'utilisation de ces deux technologies en même temps, sur les performances des réseaux dans le cas où ils ne sont pas bien configurés. Dans [93], les auteurs proposent des recommandations qui assurent un niveau acceptable de performance de réseau :

- dans le cas de l'existence d'interférences avec [WiFi](#), un décalage de 7 Mhz de la fréquence de 802.15.4 par rapport à la fréquence centrale est recommandé,
- dans le cas de l'utilisation du même canal, une séparation physique de 8 mètres entre l'interface [IEEE 802.15.4](#) et l'interface [IEEE 802.11](#) est recommandée,
- la nécessité d'utiliser les canaux [WiFi](#) 1, 7 et 13 pour l'Europe (1, 6, 11 pour l'Amérique de nord) afin d'éviter déjà les interférences intra [WiFi](#).

Une autre piste est possible pour nous, elle consiste à choisir une interface [IEEE 802.11](#) fonctionnant sur la bande des 5 GHz (c'est souvent le cas avec les interfaces [IEEE 802.11n](#) ou [.11ac](#) actuelles), et/ou utiliser des fréquences alternatives sur l'interface [IEEE 802.15.4](#), à ajuster en fonction de la région de déploiement (315 MHz, 433 MHz, 868 MHz ou 915 MHz). Si les deux interfaces [IEEE 802.11](#) et [IEEE 802.15.4](#) utilisaient une bande alternative, l'interface [ANT](#) serait seule sur la bande des 2.4 GHz.

2.3.5 Les limites de la solution proposée

Comme toute proposition, notre approche présente plusieurs limites qui doivent être identifiées et devront être résolues dans le futur.

Parmi les limites de notre solution, nous trouvons le nombre réduit de nœuds qui peuvent utiliser la période [CFP](#) (sept nœuds au maximum) par [CMAP](#), ce qui nous oblige à multiplier les [CMAP](#) dans tout le réseau pour augmenter la disponibilité de [GTS](#) à tout trafic à [QoS](#).

Le débit d'un lien classique sur [IEEE 802.15.4](#) (2.4 GHz, [DSSS](#), [OQ-PSK](#)) ne dépasse pas 250 kbits/s. Ce débit représente une lacune forte pour notre approche mais peut être résolu par l'utilisation des nouvelles améliorations de la norme [IEEE 802.15.4](#) qui offrent

des débits intéressants (en particulier 802.15.4a [94]). Néanmoins, le prétraitement effectué dans chaque canne nous permet de réduire la quantité de données émises en radio par ces dernières. Un débit de 250 kbits/s devrait être alors suffisant.

Il serait intéressant de chercher une solution qui permette à un nœud d'avoir plusieurs réservations dans plusieurs points d'accès en particulier pour les données instantanées temps réel. Ce problème est sensible en particulier dans les zones de surveillance à forte densité de cannes, comme les EHPAD. La problématique est moindre dans notre objectif initial de maintien à domicile où une seule (ou deux) personne(s) est présente, avec un nombre limité de cannes.

2.4 Architecture protocolaire

2.4.1 Présentation détaillée de notre solution

Le rôle principal de cette nouvelle fonctionnalité identifiée est de différencier les trafics générés par les applications liées aux différents capteurs de la canne, et les envoyer vers les files d'attente adéquates de l'empilement protocolaire de l'interface IEEE 802.15.4. Cette couche intermédiaire (cf. fig. 2.7) détecte également la présence d'une trame d'alerte et informe les applications par le passage vers un nouvel état nommé état critique, qui signifie que tous les capteurs doivent changer leurs caractéristiques par celles de l'état critique.

Lorsque la sous-couche de différenciation reçoit une trame, elle la place dans l'une des files d'attente. Les contenus des files d'attente seront servis dans la période de transmission adéquate (CAP ou CFP).

La sous-couche proposée contient deux composants importants :

- *Dispatcher* :
 - Il est le responsable de la classification des trames selon leurs profils,
 - chaque trame contient un champ qui indique le profil et l'application.
- *Management* :
 - la sous-couche *management* permet la sélection de la file d'attente et la synchronisation entre les trames transmises vers la sous-couche MAC et la période courante (CAP ou CFP). Elle organise les transmissions des différentes trames des files d'attente dans la période associée,
 - cette sous-couche contient trois types de files d'attente :
 - * une file d'attente dédiée aux profils qui n'ont pas de contrainte temporelle,
 - * une file d'attente pour les profils qui ont une contrainte de temps, comme les profils audio et appel d'urgence. Les trames de ce type de file seront transmises dans la période CFP.

- * une file d'attente dédiée pour les trames d'alerte.

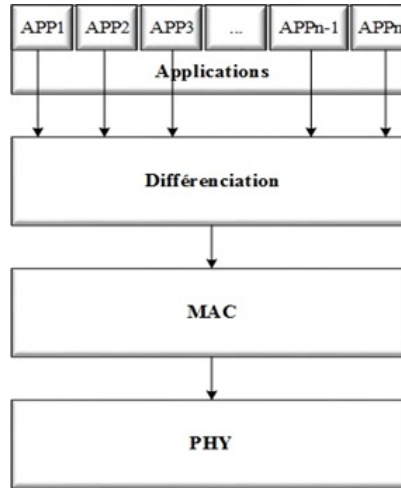


FIGURE 2.7: La position de la sous-couche de différenciation

La figure 2.7 illustre le cas de la présence de plusieurs applications hétérogènes (différents capteurs). La couche différenciation doit se situer entre la couche application et la sous-couche MAC 802.15.4, ce qui donne la possibilité de gérer et d'organiser les messages avant d'être pris en charge par la sous-couche MAC.

Dans la section 2.2.3, nous avons classifié les capteurs en 8 profils (sans prendre en considération les profils 9 et 10). Si nous associons à chaque profil une file d'attente, le nombre de files qui doivent être créées au niveau de la couche différenciation sera égal à 8. Ce nombre élevé complique les différentes étapes de traitements des messages reçus. Nous avons identifié des ressemblances au niveau de la procédure de gestion des 8 profils. A partir du tableau 2.3 précédemment présenté, nous avons remarqué que les différents profils peuvent être traités selon les périodes de transmission : CAP, CFP ou CAP/CFP. Le nombre minimal de files d'attente qui doit être créée dans la couche différenciation est donc égal à trois. Chaque file d'attente permet à ces trames de bénéficier d'un service précis. Ces services sont définis dans la couche différenciation et sont accordés selon les besoins de chaque file. Ce constat simplificateur nous a imposé de nouveau la création de profils équivalents à partir des profils identifiés dans le chapitre 2.2.3. Ceci représente une solution pour diminuer le nombre de files d'attente et pour simplifier le traitement. Les profils équivalents représentent les profils qui utilisent la même période de transmission. Le nombre de profils équivalent que nous avons déduit est égal à trois :

- **profil équivalent des messages tolérants** : il contient les profils qui sont tolérants à la latence. Ils sont envoyés vers le CMAP dans la période CAP. Les trames sont envoyées vers la *File des Messages Tolérants (FMT)*,
- **profil équivalent des messages temps réel** : il contient les profils qui ne sont pas tolérants à la latence et ils sont transmis vers le CMAP dans la période CFP. Les trames sont envoyées vers la *File des Messages temps Réel (FMR)*,

- **profil équivalent des messages d'urgence** : il contient les profils qui doivent être transmis dans les deux périodes **CAP** et **CFP**. Les trames sont envoyées vers la *File des Messages Urgents* (**FMU**).

La figure 2.8 illustre un exemple qui explique ce cas :

- le capteur de température de la main et le capteur **TOR** appartiennent aux profils 2 et 3 respectivement. Ainsi, ils appartiennent au profil équivalent tolérant,
- l'accéléromètre appartient au profil 5 et donc au profil *équivalent temps réel*,
- une trame d'alerte appartient au profil 9. Elle représente une indication sur la dégradation d'un paramètre médical vital, ce qui peut être un passage vers une situation critique. Ce message appartient au profil équivalent urgent.

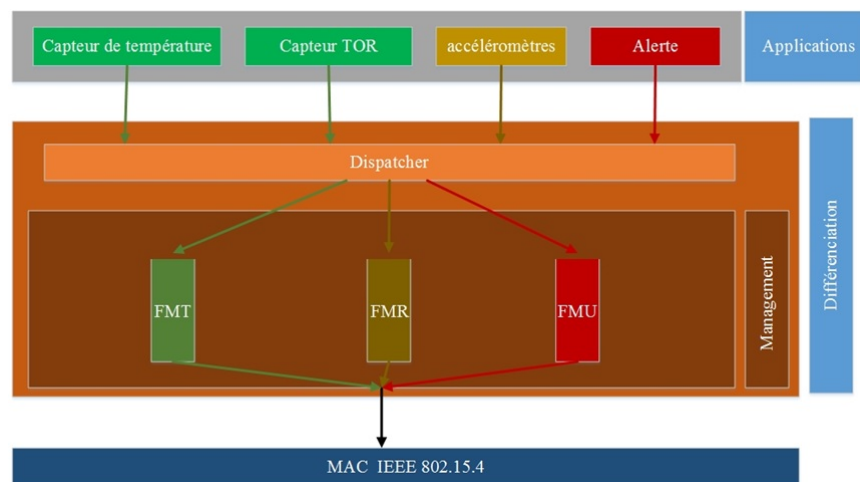


FIGURE 2.8: Composants de la couche différenciation

Les trafics générés par les applications sont traités par la sous-couche *dispatcher* lors de leur réception. Ensuite, ils sont dirigés vers les files d'attente adéquates à leurs profils. La transmission des trames vers la sous-couche MAC 802.15.4 s'effectue par la sous-couche management qui servira les trames des files d'attente selon la période **CAP** ou **CFP** adéquate à l'instant donné.

La figure 2.8 représente le cas d'utilisation de trois capteurs avec la présence d'une trame d'alerte. Les trafics générés par les capteurs d'humidité et **TOR** appartiennent au même profil équivalent, ce qui signifie qu'ils sont tolérants à la latence et qu'ils exigent le même traitement au niveau de la sous-couche management. Les trames de ces deux capteurs seront envoyées vers la file d'attente **FMT**.

L'accéléromètre n'appartient pas au même profil équivalent des deux autres capteurs. Le trafic généré ne peut subir le même traitement. Pour cette raison, lorsque la couche dispatcher reçoit ses trames, elle les place dans la file d'attente **FMR**.

Le message d'alerte représente un cas spécifique puisqu'il doit être transmis dans les plus brefs délais, pour cette raison nous lui avons associé une file d'attente spécifique.

A partir de l'explication présentée dans le paragraphe précédent, nous pouvons définir les caractéristiques associées à chaque file d'attente :

- **FMU** :
 - c'est une file très prioritaire,
 - elle empêche toutes les autres transmissions, si elle n'est pas vide,
 - elle ne contient que les trames d'alerte,
 - les trames de cette file d'attente sont transmises dans les périodes **CAP** et **CFP**.
- **FMR** :
 - c'est une file d'attente pour les messages avec une contrainte temporelle,
 - elle a une priorité plus faible que **FMU** et plus forte que **FMT**,
 - les trames de cette file seront servies dans la période **CFP**.
- **FMT** :
 - c'est la file qui reçoit les trames qui n'ont pas de contrainte temporelle,
 - les trames de cette file sont transmises dans la période **CAP**.

Dans cette section, nous avons présenté notre solution de différenciation avec des détails sur l'architecture de cette nouvelle couche. Dans la section suivante, nous présenterons le fonctionnement de la couche différenciation lors de la réception d'une trame qui appartient à l'un des profils équivalents.

2.4.2 Traitement des profils équivalents par la couche différenciation

Lors de la réception d'une trame, la couche *dispatcher* va vérifier son entête. Chaque trame appartient à un profil qui est inclus dans le profil équivalent. Selon le profil équivalent, la sous-couche *dispatcher* décide à quelle file d'attente la trame appartient.

Les trames du profil équivalent des messages tolérants et des messages temps réels seront transmises dans la période **CAP** et **CFP** respectivement. La sous-couche *management* est la responsable de la sélection de la file d'attente selon la période de transmission courante.

Les trames du profil équivalent des messages d'urgences sont envoyées vers la file **FMU**. La sous-couche *dispatcher* génère un message de notification qui sera envoyé vers les couches supérieures. Ce message autorise les applications à changer leurs caractéristiques

courantes par celles correspondant au profil 10. De même, la sous-couche dispatcher informe la sous-couche management de la présence d'une trame dans la file [FMU](#). Dès la réception de l'indication, la sous-couche management arrête de servir les autres files d'attente et traite les trames de la file [FMU](#). Les trames de cette file seront transmises dans les périodes [CAP](#) et [CFP](#).

Lors de la présentation des profils équivalents, nous n'avons pas considéré le cas du profil 6 (profil du bouton d'appel d'urgence). Ce profil 6 n'appartient à aucun profil équivalent. En effet, ce profil génère une interruption matérielle qui sera traitée directement par la sous-couche management. De cette façon, le temps de traitement sera le plus rapide, et sans incidence si les files d'attente sont déjà bien remplies. Lorsque la sous-couche management reçoit l'interruption matérielle, elle génère une trame de réservation de ressources nécessaires pour la transmission des messages du profil 4. La trame générée représente l'initiation de l'établissement d'une communication temps réel. Elle réservera donc les ressources nécessaires pour ce type de communication. L'indicateur sur l'acceptation ou le refus de la réservation sera inclus dans le *beacon* envoyé par le [CMAP](#).

2.4.3 Présentation des messages et des primitives associées

Dans notre architecture, trois types de messages peuvent être générés et traités par la couche différenciation :

- des messages de données,
- des messages d'alerte,
- des messages de notification.

Dans cette section, nous présenterons les différents messages et les diagrammes de séquences associés.

2.4.3.1 Messages de données

Les messages de données contiennent les informations collectées par les capteurs. La taille du champ de données varie d'un capteur à un autre. Le message contient les champs suivants :

- type de message,
- profil,
- identifiant de l'application,
- données.

Lorsqu'une application envoie un message, elle inclut dans l'entête du message son profil et son identifiant. À la réception d'un message, le dispatcher vérifie l'entête, puis transmet le message vers la file d'attente adéquate. La couche management connaît toutes les informations nécessaires pour qu'elle puisse transmettre les messages dans les périodes prédéfinies. Donc, lorsque la période CAP commence, la couche management commence l'envoi des trames en attente dans FMT. De même, lorsque la période GTS associée au nœud commence, la couche transmet les trames de FMR (cf. figure 2.9).

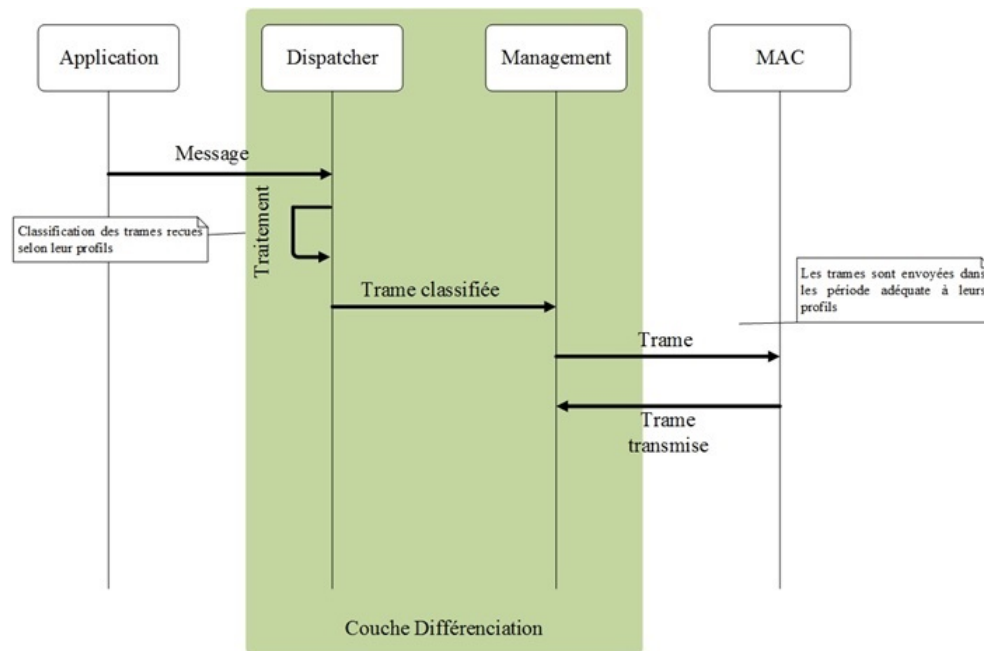


FIGURE 2.9: Séquence de transmission des messages

2.4.3.2 Message d'alerte

L'alerte est un message envoyé par une application qui détecte une évolution anormale des données capturées. Cet état d'alerte doit être géré au plus vite sous peine d'éviter tous problèmes graves à la santé de la personne. La structure du message d'alerte est la même que celle utilisée pour les messages de données.

Lors de la réception d'un message d'alerte, le dispatcher informe la couche management de la présence d'un message de très haute priorité qui doit être traité immédiatement par l'envoi d'un message de notification. Ainsi, le dispatcher envoie une notification aux applications pour activer l'état critique.

Lorsque la sous-couche management reçoit cette notification, elle termine la transmission du paquet courant vers la sous-couche MAC et commence à transmettre les trames de FMU. La trame d'alerte doit être transmise dans les périodes CAP et CFP afin d'augmenter les chances que la trame soit bien reçue et le plus rapidement possible.

Lors de la transmission de la trame d'alerte, deux cas peuvent être présents :

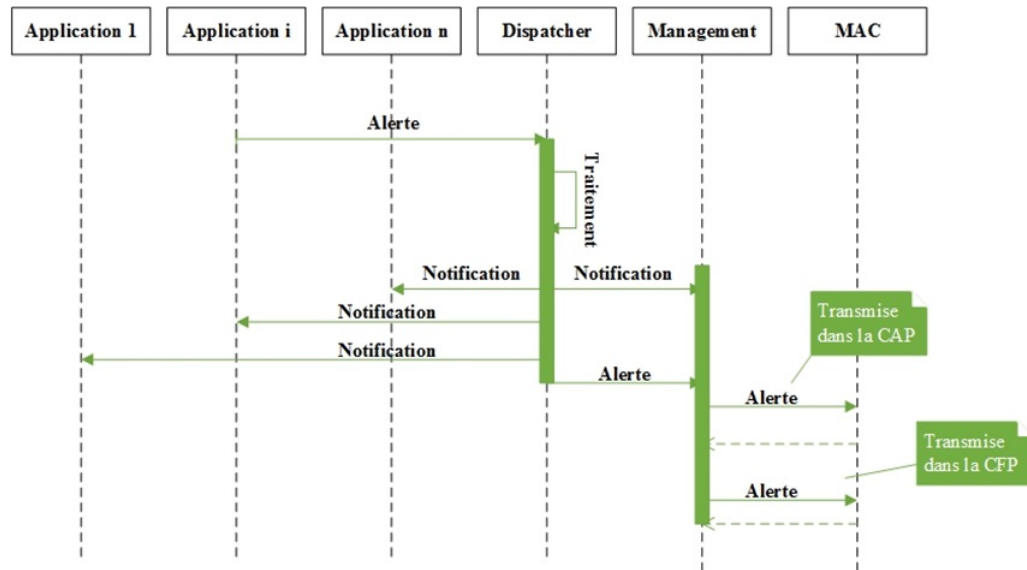


FIGURE 2.10: Traitement du message d'alerte

- La trame est présente dans la CAP présente avant la CFP (cf. figure 2.10) : dans ce cas, la trame d'alerte sera transmise dans la même supertrame. La transmission de la trame dans la période CAP n'est pas certaine. Donc, il est possible que la trame transmise dans la CFP soit transmise avant celle de la CAP si le nœud n'obtient pas l'opportunité d'accéder au medium,
- La trame est présente dans la CFP présente avant la CAP : dans ce cas, les trames d'alerte seront transmises dans deux supertrames différentes.

2.4.3.3 Messages de notification

La notification est une trame créée et envoyée par la sous-couche dispatcher vers les applications et la sous-couche management. Cette trame de notification contient les champs suivants :

- type de message,
- données.

Lorsque les applications reçoivent un message de notification, ils changent les caractéristiques actuelles utilisées par celles du profil 10.

L'augmentation du nombre de trames à transmettre dans les périodes CAP et CFP peut engendrer un débordement des files d'attente. Aussi, l'importance du suivi dans le cas d'état critique rend la canne qui génère cette alerte plus prioritaire que d'autres cannes dans le réseau. Pour ces raisons, lorsque la sous-couche *management* reçoit la trame de notification, elle change la valeur de BE (*Backoff Exponent*) utilisée par l'algorithme CSMA/CA en la divisant par 2. Cette nouvelle valeur de BE permet à

la canne à laquelle correspond l'état critique d'avoir la priorité d'accès au médium, ce qui permet d'éviter ou de réduire les pertes des trames au niveau de la file d'attente à cause du débordement. Aussi, lorsque la sous-couche *management* du coordinateur reçoit la notification d'alerte, elle recalculera les valeurs de **BO** et **SO** selon les nouveaux paramètres (les services offerts par chaque nœud sont enregistrés dans la sous-couche *management*). Les nouvelles valeurs de **BO** et **SO** seront envoyées dans la prochain *beacon* avec une indication sur la présence d'un état d'alerte dans une canne du réseau.

Nous sommes ici en train de définir un nouveau type de priorité utilisée au niveau des cannes. Au départ, tous les nœuds ont le même niveau de priorité. Ils ont donc la même opportunité pour accéder au médium et transmettre les données vers le coordinateur (figure 2.11). Dans la figure 2.11, par exemple, nous avons 4 cannes. Chaque canne dispose d'une priorité d'accès au réseau. Dans l'état initial, toutes les cannes ont le même niveau de priorité (noté ici P0).

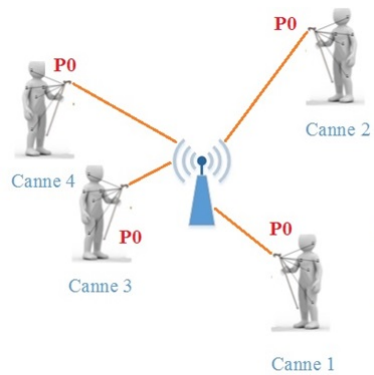


FIGURE 2.11: Cas d'un réseau dans l'état initial

Nous supposons que nous avons un état d'alerte pour la canne 2, ce qui va influencer les performances du réseau par l'augmentation du nombre des trames envoyées. Puisque la canne 2 est en état d'alerte, sa sous-couche *management* demande à diminuer la valeur de **BE** pour avoir plus de chance d'accéder au médium dans la période **CAP** et la couche *management* envoie les nouvelles valeurs de **BO** et **SO** à la couche *MAC* pour les transmettre dans le *beacon*. Dès la réception du *beacon*, les cannes mettent à jour tous les paramètres utilisés. Ce changement se traduit par l'attribution de la priorité P1 à la canne 2.

Lorsque le coordinateur reçoit un message d'alerte, il informe les autres nœuds du réseau dans le *beacon* suivant. Dès que les nœuds qui n'ont pas déclenché l'alerte reçoivent l'indication de l'existence d'un état critique déclenché par un nœud de réseau, la couche *management* commence le suivi des valeurs de *Backoff* tirés à chaque essai de transmission. Si cette valeur est inférieure à $2^{\frac{BE}{2}}$ alors la couche *MAC* la décale de $2^{\frac{BE}{2}}$ afin d'avoir une valeur de *Backoff* plus grande que celle du nœud en état critique (cf. Figure 2.12).

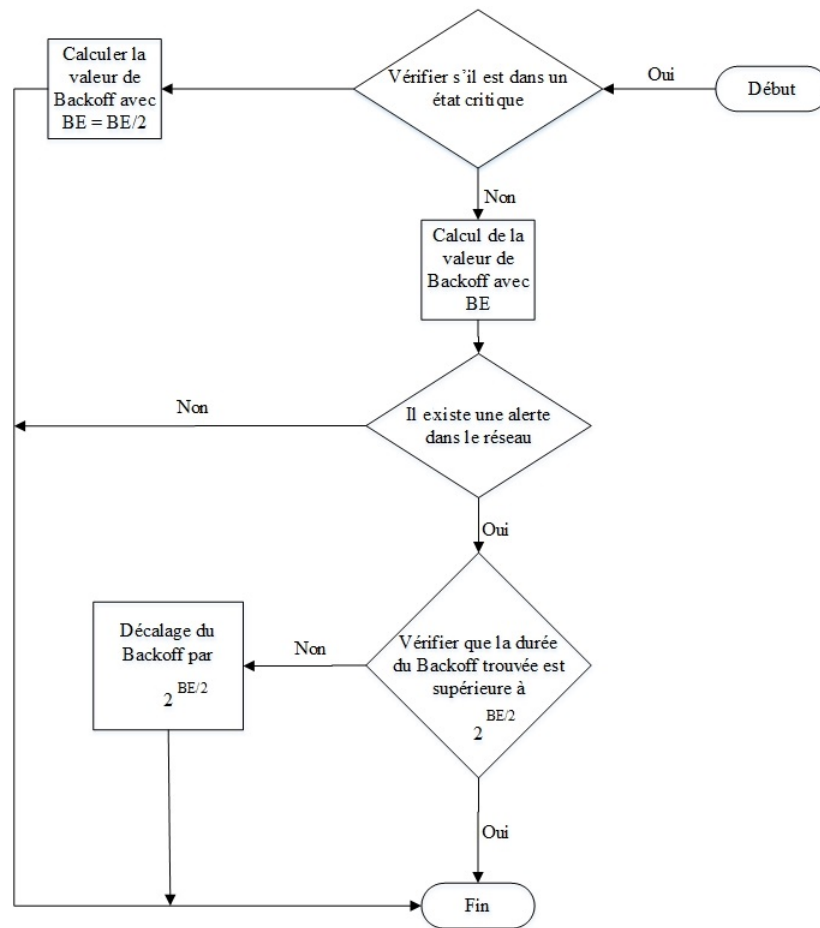


FIGURE 2.12: Diagramme d'activité de calcul du Backoff

2.4.3.4 Communication audio

Les échanges vocaux sont très importants dans le cas d'urgence où la personne âgée a besoin d'aide. Le projet *CANet* offre cette fonctionnalité par l'intégration d'un haut-parleur et d'un microphone dans la canne. Dans cette section, nous détaillons le processus d'établissement d'une communication vocale à travers la norme [IEEE 802.15.4](#) avec le mode Beacon. Ce processus contient quatre étapes :

1. Appui sur le bouton d'appel d'urgence, ce qui génère une interruption matérielle,
2. Réservation des ressources pour la communication voix,
3. Acceptation de la demande d'appel,
4. Notification à la couche application pour le bon déroulement des étapes 2 et 3 et donc, début de la communication vocale.

A partir des étapes présentées, nous pouvons déduire que les profils 4 et 6 sont liés. Le profil 4 est l'initiateur du processus de la communication vocale.

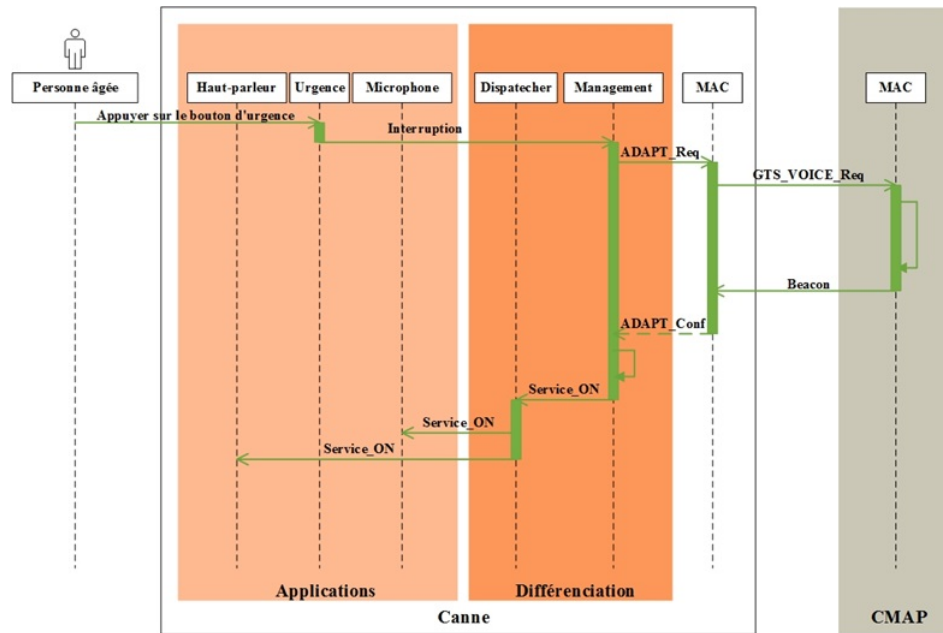


FIGURE 2.13: Initialisation de transmission de message de profil 4 côté canne (cas sans refus de la demande)

Lorsque la sous-couche management reçoit une interruption matérielle, elle génère la primitive `ADAPT_req`. Cette primitive est envoyée à la sous-couche MAC qui envoie la commande `GTS_VOICE_Req` demandant la réservation de 4 slots `GTS`, deux slots pour la réception et deux slots pour la transmission dans le cas de l'utilisation de `codec Opus` (cette partie sera expliquée dans la section 2.6), dédiée pour la communication audio. Elle sollicite également, côté `CMAP`, l'adaptation des valeurs de `BO` et `SO` aux caractéristiques du profil 4.

La réception de la commande `GTS_VOICE_Req` de la part de la couche MAC de `CMAP` représente le déclencheur qui lance le processus. Le message de demande de réservation sera transmis une seule fois au début de la communication de demandeur de la communication jusqu'au centre de contrôle. La demande de réservation des slots `GTS` sera transmise dans la `CFP` ce qui nous assure que la demande est bien reçue par le `CMAP`.

La couche application responsable de la communication au niveau du centre de contrôle est la seule autorisée à prendre la décision d'acceptation ou de refus de la demande de l'établissement de la communication audio. Si l'un des personnels de centre de contrôle accepte la demande de communication vocale, la couche application envoie un message de confirmation qui mentionne l'acceptation de l'établissement de la communication. Donc, la sous-couche management reçoit la primitive de confirmation nommée `Service_conf`. La sous-couche MAC reçoit le primitive `ADAPT_ind`, elle procède donc à la transmission de cette commande à travers le lien 802.15.4 vers la canne qui demande la communication.

Si la sous-couche MAC ne reçoit pas la commande `ADAPT_ind` pendant un certain temps, elle ne change rien au niveau des paramètres et elle n'effectue pas la réservation (la demande est refusée par les couches supérieures du centre de contrôle). Finalement,


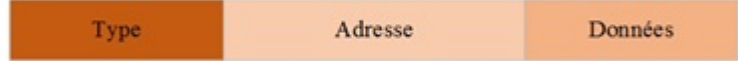

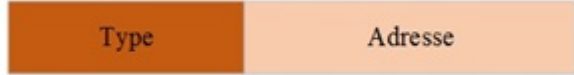
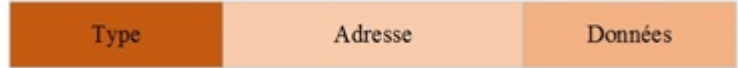

Primitives et messages	Structure
ADAPT_req	
ADAPT_conf	
GTS_VOICE_req	
Service_on	
Service_Req	
Service_conf	
ADAPT_ind	

TABLE 2.4: Primitives et messages nécessaires pour l'établissement d'une communication vocale

la sous-couche MAC de **C**MAP envoie un beacon qui contient la réponse des couches supérieures du centre de contrôle.

Lorsque la sous-couche MAC de la canne demandeuse reçoit le beacon, elle vérifie si les paramètres **B**O et **S**O sont changés et s'il existe une réservation du nombre de slots demandés. Si elle identifie les valeurs adéquates de **B**O et **S**O, elle informe la sous couche management par le primitive ADAPT_confirm avec la valeur *True*. La sous-couche management informe alors la couche applicative responsable que la demande est acceptée par la primitive Service_ON. Dans le cas contraire, la sous-couche management reçoit la primitive ADAPT_confirm avec une valeur *False*.

Les structures des différentes primitives utilisées pour l'établissement d'une communication audio sont présentées dans le tableau 2.4.

Dans cette partie, nous avons supposé que l'acceptation de communication s'effectue par les applications de **C**MAP, mais en réalité, c'est une application distante qui va accepter la communication et la réservation sera validée en retour du message de confirmation. Donc, dans le cas réel, nous avons trois étapes :

1. étape de réservation de ressources nécessaires pour la communication audio,
2. étape de validation des nouveaux paramètres et de réservation dans le cas de l'acceptation de l'établissement de la communication vocale,

3. étape d'annulation des réservations effectuées dans le cas de refus de la communication vocale.

2.4.3.5 Demande de libération de la période CAP suivante

Pendant le fonctionnement du système dans les cannes, nous pouvons être en présence d'un état critique. Dans cet état, nous avons une augmentation du nombre de messages générés par les applications. Cette augmentation peut saturer les files d'attente. Il y a une forte probabilité de rejet de plusieurs messages, ce qui peut influencer négativement les analyses de données effectuées côté récepteur final. Pour résoudre ce problème, nous avons décidé de donner la possibilité à la sous-couche management de demander la libération de la période CAP dans la supertrame 802.15.4 suivante.

La figure 2.14 présente les étapes effectuées lors d'une demande de libération de la CAP. La sous-couche management envoie une demande LIB_CAP_req qui sera traitée par la sous-couche MAC du CMAP. La réponse à cette demande sera envoyée dans le beacon suivant. Lorsque la sous-couche MAC reçoit la réponse, elle émet le message de commande LIB_CAP_conf avec une réponse *True* ou *False* pour indiquer si le CMAP a accepté ou refusé la demande.

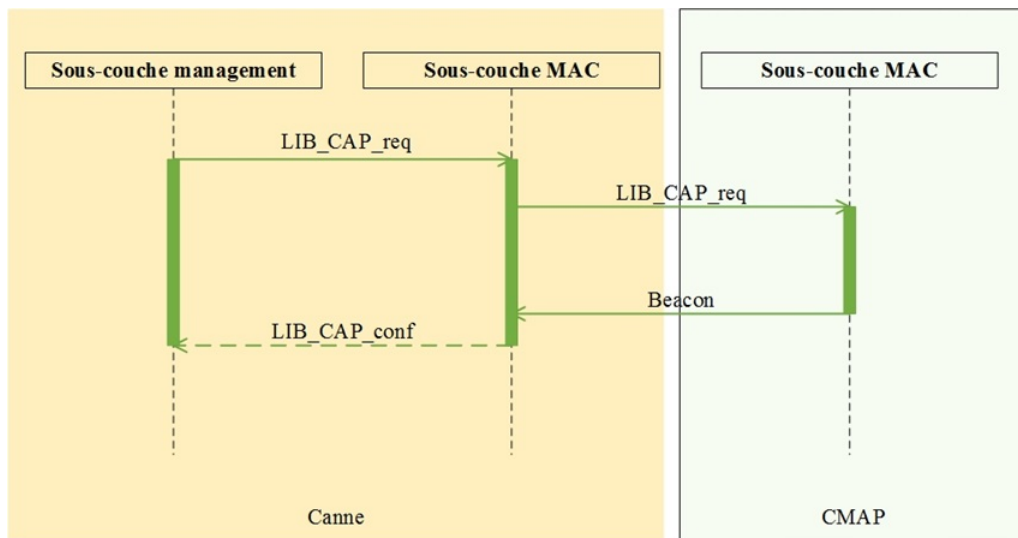


FIGURE 2.14: Demande de libération de la période CAP

Dans cette section, nous avons présenté nos propositions protocolaires en les illustrant par les scénarios principaux, et nous avons défini le format des messages et les primitives de notre couche de différenciation. Dans la section suivante, nous présentons l'automate d'états de notre couche de différenciation.

2.4.4 Diagramme d'état

Les changements d'état dépendent des files d'attente et de la présence d'une interruption matérielle à l'instant t . Pour passer d'un état à un autre, il faut avoir un état des files d'attente bien précis défini par les paramètres suivants :

- **EFMU** qui représente l'état de la file d'attente de très forte priorité,
- **EFMR** qui représente l'état de la file d'attente de forte priorité,
- **EFMT** qui représente l'état de la file d'attente de faible priorité,
- **IM** qui représente la réception d'une interruption système.

Les paramètres **EFMT**, **EFMR** et **EFMU** sont à **True** (**T**) si il existe au moins un message dans la file d'attente, sinon ils sont mis à **False** (**F**). Le paramètre **IM** est égal à **T** si il existe une interruption matérielle sinon il est égal à **F**.

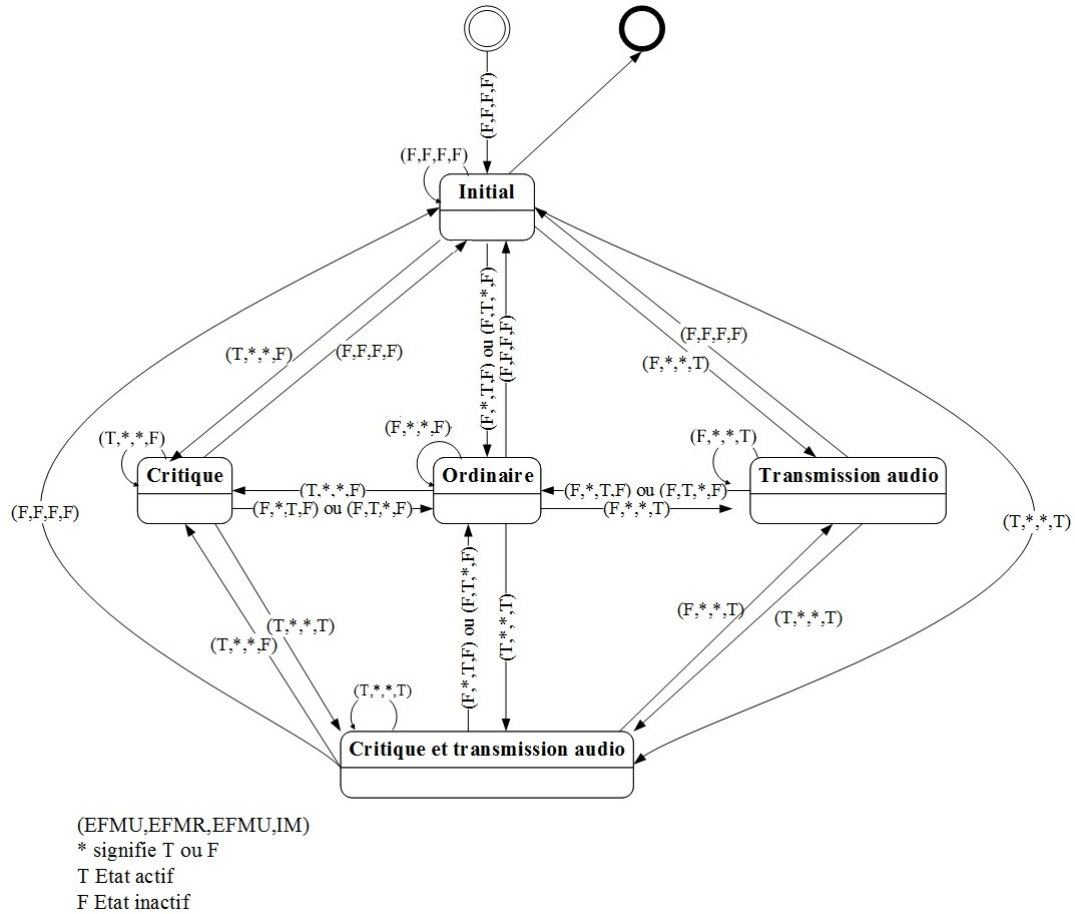


FIGURE 2.15: Automate d'état de la couche différenciation

La signification des états représentés dans la figure 2.15 est la suivante :

- **initial** : dans cet état, la sous couche de différenciation attend la réception d'un message de la part des applications (capteurs).

- **ordinaire :**

- transmission périodique des messages qui sont dans les files **FMT** et **FMR**. Les messages sont transmis respectivement dans les périodes **CAP** et **CFP**
- les valeurs de **BO** et **SO** sont **BO_{ini}** et **SO_{ini}** fixées par le coordinateur lors de l'émission de son premier beacon.

- **critique :**

- une demande est envoyée aux applications pour accélérer la transmission des informations de contrôle.
- la valeur de **BE** est changée en **BE1** avec $BE1 < BE$ pour le nœud qui contient un état critique. Les autres nœuds du réseau ne changent pas la valeur de **BE** mais ils effectuent un décalage de 5 symboles lorsque la valeur de Backoff calculée est inférieure à 5 symboles,
- la couche différenciation recalcule les valeurs de **BO** et **SO** selon les nouveaux paramètres de réseau. Cette valeur sera envoyée dans le prochain beacon avec une indication qui informe les nœuds du réseau de l'obligation d'utiliser les nouveaux paramètres.

- **transmission audio :**

- dans cet état, la canne transmet des trames vocales vers le **CMAF** et reçoit aussi des trames audio envoyées par le **CMAF**.

Dans cette section, nous avons présenté l'architecture de la couche différenciation. Aussi nous avons détaillé le fonctionnement de deux sous couches dispatcher et management pour chaque type de profil et les différents états possibles. Dans le chapitre suivant, nous présenterons l'étude théorique de **BO** et **SO**. Cette étude nous aidera à choisir les bonnes valeurs de **BO** et **SO** pour chaque profil.

2.5 Etude théorique de BO et SO

Dans les précédentes sections, nous avons présenté la classification des profils et notre solution pour la différenciation. Chaque profil est caractérisé par une périodicité et un débit différents. Cette hétérogénéité rend le choix des paramètres **BO** et **SO** difficile.

L'un de nos objectifs et point important de notre contribution est de ne pas reconstruire entièrement une couche MAC mais de nous baser sur les leviers disponibles et offerts par la norme, en particulier les paramètres **BO** et **SO**, en jouant sur la taille de la supertrame qui est configurable, mais que peu de contributions ont exploité. D'après ce que nous avons présenté dans le chapitre 1, la durée d'une supertrame dépend essentiellement de deux paramètres : **BO** et **SO**. La variation de ces deux paramètres a une influence sur la durée de la **CAP** et de la **CFP**. Ceci influence également la durée d'attente des trames

des files [FMR](#) et [FMT](#). L'importance de ces deux paramètres nous a encouragé à étudier l'impact de [BO](#) et [SO](#) sur les performances réseau, tels que le débit théorique, la durée de la supertrame... afin de proposer des valeurs adéquates à chaque profil.

2.5.1 Variation du débit en fonction de BO et SO

Comme nous l'avons rapidement évoqué précédemment, notre solution de différenciation se base sur l'utilisation de la topologie étoile, avec le mode beacon de [IEEE 802.15.4](#). Le choix de cette configuration est effectué afin d'obtenir la période [CFP](#) qui offre la garantie de [QoS](#). Le projet *CANet* contient des applications qui exigent un certain niveau de [QoS](#). Ce qui rend l'utilisation de [CSMA/CA](#) dans la période [CAP](#) peu adaptée à notre cas. La norme [IEEE 802.15.4](#) exige l'utilisation du mode beacon afin de rendre possible l'utilisation de la [CFP](#). L'utilisation du mode beacon n'est possible que dans la topologie étoile puisque le beacon est créé par le coordinateur de réseau [P1].

Les valeurs sélectionnées de [BO](#) et [SO](#) permettront de classer des trafics et de satisfaire ainsi l'exigence de tous les types de trafic [P1].

Nous calculons le *Débit Théorique Moyen* ([DTM](#)) :

$$DTM = \frac{SD}{BI} \frac{\text{symboles}}{\text{symboles}} \times 250 \frac{\text{Kbit}}{s} = \frac{1}{2^{BO-SO}} \times 250 \frac{\text{Kbit}}{s} \quad (2.1)$$

La figure 2.16 illustre l'équation (2.1). Elle représente la variation du débit théorique moyen en fonction des différentes valeurs de [BO](#) et [SO](#). Si [BO](#) et [SO](#) sont égaux, le débit théorique moyen est égal à 250 kbit/s. Si les valeurs de [BO](#) et [SO](#) sont différentes ($SO < BO$), le débit théorique moyen diminue.

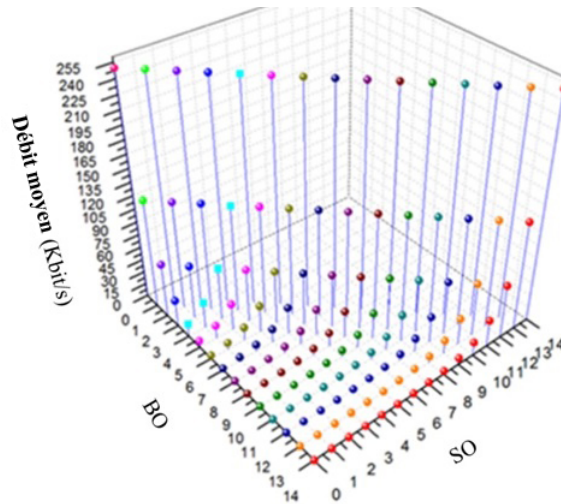


FIGURE 2.16: Débit moyen en fonction de BO et SO

Dans la figure 2.17, la supertrame a la plus grande durée et le plus grand débit théorique moyen lorsque $BO = SO$, $\forall BO$ et $\forall SO$. Si les valeurs de [BO](#) et [SO](#) ne sont pas

identiques, la durée de supertrame diminue et le débit théorique moyen devient plus faible (figure 2.18). Dans ce cas, nous avons l'apparition de la période inactive.

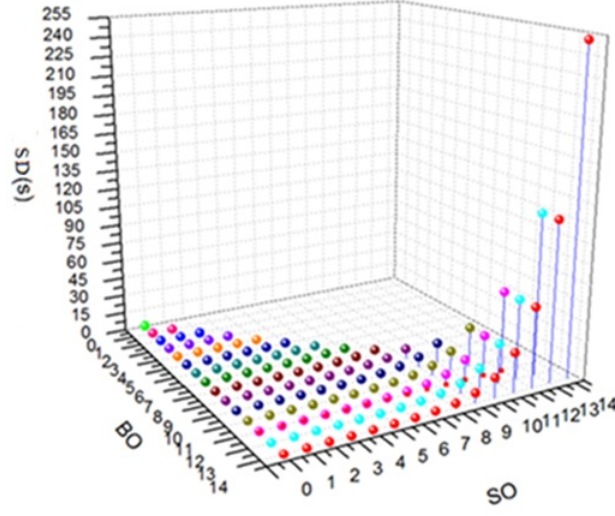


FIGURE 2.17: Variation du superframe duration (SD) en fonction de BO et SO

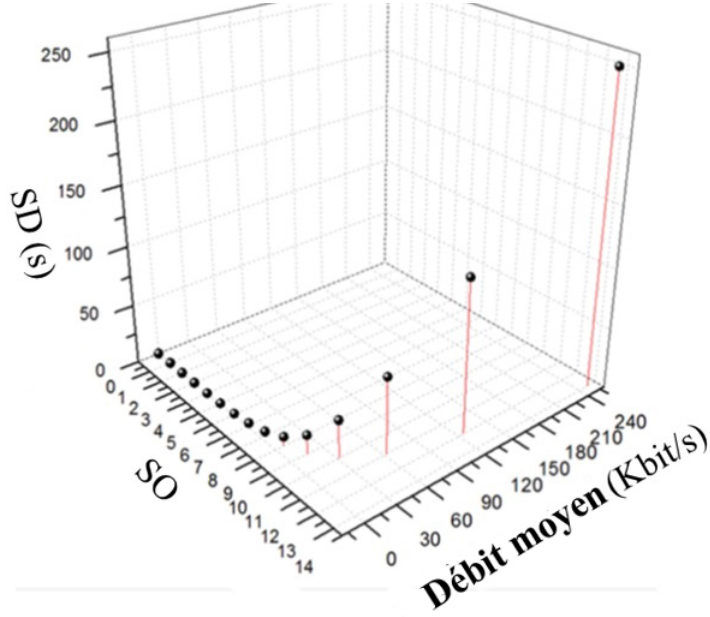


FIGURE 2.18: Variation du superframe duration en fonction de SO et du débit moyen avec $BO = 14$

La durée de la période inactive est calculée par :

$$Période\ Inactive = BI - SD = 960 \times (2^{BO} - 2^{SO}) \times 16 \times 10^{-6}s \quad (2.2)$$

La figure 2.19 représente la variation de la période d'inactivité en fonction de $BO - SO$ et de BO . La valeur de SO varie de 0 à BO . Si la valeur SO est égale à 0, la longueur de la période inactive est égale à la longueur de BI . Dans les autres cas, la durée de la

période inactive diminue lorsque la valeur de $BO - SO$ augmente. Donc, la durée de la période inactive dépend essentiellement de la valeur de SO .

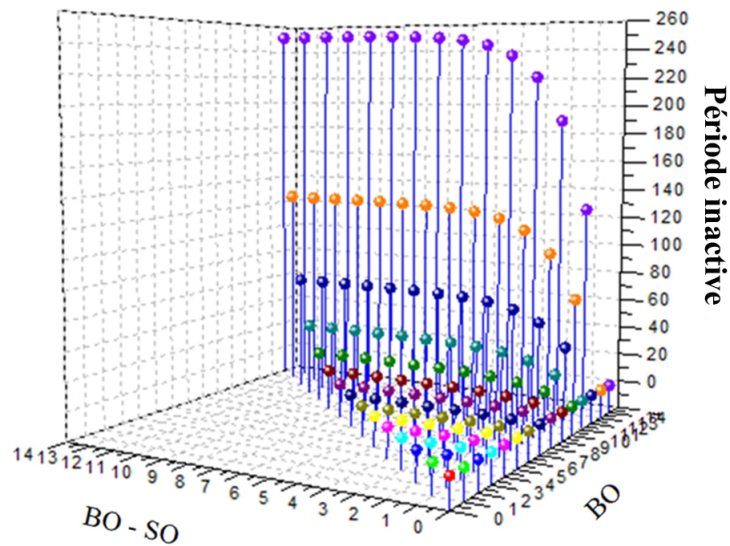


FIGURE 2.19: Variation de la durée inactive en fonction de BO et de $BO - SO$

2.5.2 Choix des valeurs de BO et SO

Les figures 2.16, 2.17, 2.18 et 2.19 peuvent nous aider à compléter l'étude sur les profils en rajoutant des valeurs théoriques optimisées de BO et SO pour les différents profils. Dans le tableau 2.5, nous avons associé à chaque profil les valeurs de BO et SO les plus adaptées et obtenues par notre étude. Nous avons également rajouté des informations concernons le délai typique, $BO - SO$ et le nombre de trames transmises dans chaque supertrame pour les différentes valeurs de BO et SO choisies (périodicité en terme de supertrame).

Capteur	Profils	BO	SO	BO-SO	Durée d'une supertrame	Durée de BI	Débit moyen (kbit/s)	Délai typique entre les trames	Période	Périodicité en termes de supertrame							
Capteur de prise de main en main	1	Ne dépend pas des valeurs fixes de BO et SO mais il faut avoir au moins une et pas plus de 10 trame/s								CAP	Aucune périodicité						
Capteur de température de la main	2/9/10	Variée de 0 à 14	[0..14]	[0..14]	[15 ms..252 s]	[15 ms..252 s]	[15,3..250]	Chaque 4 min			[1..9600] (chaque 4 min) [1..40000] (chaque 10 min)						
Capteur de température extérieure																	
Capteur d'humidité								Chaque 10 min									
Capteur d'humidité de corps humain	2/9							Typiquement 2 fois par seconde, s'il n'existe pas de variation les capteurs				[0..33]					
Capteur de la charge de batterie								Sécurité système cardiaque. Typiquement chaque 20 ms									
Capteur TOR	3/10									CFP	Dans chaque supertrame						
Capteur de rythme cardiaque	8/9/10																
Microphone Haut-parleurs	3	3	3	0				30 ms									

Capteur	Profils	BO	SO	BO-SO	Durée d'une supertrame	Durée de BI	Débit moyen (kbit/s)	Délai typique entre les trames	Période	Périodicité en termes de supertrame
n ou plusieurs accéléromètres	5/10	Variée de 0 à 14	[0..14]	[0..14]	[15 ms..252 s]	[15 ms..252 s]	[15,3..250]	Selon la vitesse de la personne âgée. Typiquement chaque 2 ou 3 secondes	CFP	Dans chaque supertrame
Bouton d'appel d'urgence	6	Ne dépend pas des valeurs fixes de BO et SO							CAP et CFP	Aucune périodicité
Système de localisation	7/9/10	Variée de 0 à 14	[0..14]	[0..14]	[15 ms..252 s]	[15 ms..252 s]	[15,3..250]	Chaque 4 min (envoi d'un parcours qui contient 24 points donc une position chaque 10 s)	CAP	[1..9600]
		Variée de 0 à 11	[0..6]	[0..10]	[15 ms..983 ms]	[15 ms..15,72s]	[15,3..107,14]	Chaque seconde		
Trame d'alerte	9	Ne dépend pas des valeurs fixes de BO et SO							CAP et CFP	Aucune périodicité
État critique	10	Ne dépend pas des valeurs fixes de BO et SO							CAP ou CFP	Dans chaque supertrame
									Les délais typiques des profils seront divisés par 60 secs, sauf ceux du profil 3 (il émet à chaque variation) et du profil 9 qui ne changent pas	

TABLE 2.5: Généralisation des paramètres des profils

Dans le tableau 2.5, nous avons fixé des conditions pour le profil 1 afin d'assurer la bonne gestion de trafics envoyés. Pour le profil 1, nous avons majoré le nombre de trames générées par le capteur par 10 trames/s. Cette valeur ne peut pas être atteinte par la personne âgée. Elle représente pour nous un repère qui permet de contrôler le nombre maximal de trames générées. Aussi nous avons minoré le nombre de trames générées par 1. Cette valeur permet de valider que la personne âgée a utilisé sa canne au moins une fois par jour. Dans cette section, nous avons étudié l'influence de la variation de BO et SO sur le réseau. Cette étude nous a permis de compléter le tableau de profils par les valeurs adéquates de BO et SO. Dans la section suivante, nous étudions le cas de la transmission de voix et nous fixons le codec qui sera utilisé.

2.6 Etude de la transmission de la voix

Parmi les capteurs et actionneurs utilisés dans la canne, il est prévu un microphone et un haut-parleur. Notre but est donc de transmettre une communication vocale duplex sur les liens IEEE 802.15.4.

Dans cette section, nous effectuons une étude théorique pour le choix du codec. Cette première étude nous permettra de proposer une solution originale de transmission de voix sur ce WPAN.

2.6.1 Choix du codec

Dans le domaine de la VoIP (*Voice over Internet Protocol*), plusieurs codecs sont développés pour profiter des avancées technologiques et offrir une qualité de voix acceptable avec un débit relativement faible. On trouve parmi les codecs les plus connus et les plus utilisés : Speex [95], iLBC [96], G711 [97], G723 [97], G729 [97], Opus [98]... (cf. Tableau 2.6)

Les équations suivantes sont utilisées dans les calculs réalisés [P5] :

$$Taille\ d'une\ trame = \frac{Débit\ (kbits/s) \times durée\ de\ la\ trame\ (s) \times 10^{-3}}{8} Octets \quad (2.3)$$

$$Nombre\ de\ paquets\ par\ seconde\ (PPS) = \frac{1000}{Taille\ d'une\ trame} \quad (2.4)$$

$$Taux\ d'utilisation\ (TU) = \frac{PPS}{SPS} \quad (2.5)$$

Avec :

$$SPS = nombre\ de\ supertrames\ par\ seconde = \frac{100}{durée\ d'une\ supertrame} \quad (2.6)$$

Tous ces **codecs** sont comparés par rapport aux valeurs de **BO** et **SO**, ce qui nous permet de déterminer le **codec** le plus adapté aux spécifications de la norme **IEEE 802.15.4**.

Dans cette comparaison, nous avons identifié que les débits fournis par les **codecs** varient entre 2 et 510 kbits/s [P5].

Codec	Débit (kbits/s)	Fréquence d'échantillonnage (Khz)	Durée d'un paquet (ms)	Taille d'un paquet (octets)	Nombre de paquets/s (PPS)
G.711	64	8	10	80	100
G.729	8		10	10	100
G.723.1	6.3		30	24	34
G.723.1	5.3		30	20	34
G.728	16		5	10	200
iLBC	13.33		20	34	50
	15.20		30	57	34
Speex	2.15 à 44.2	8, 16, 32 ou 48	30	8 à 188	30
			34		34
Opus (mode LP) [6]	5 à 24	8 à 48	10, 20, 40, 60	7 à 180	20 à 100
Opus (mode Hybride)[6]	20 à 48		10, 20	25 à 120	20 à 100
Opus (mode MDCT)[6]	16 à 128		2.5, 5, 10, 20	5 à 320	50 à 500

TABLE 2.6: Paramètres des codecs

Le débit fourni par le **codec** est un paramètre important pour la norme **IEEE 802.15.4** car le débit maximal sans fil théorique est égal à 250 kbits/s. Le **codec** G711 est donc délaissé, car il nécessite un débit trop important par rapport aux autres **codecs**.

Les **codecs** G729 et G728 sont éliminés de notre choix, car le nombre de paquets par seconde est trop grand par rapport aux autres **codecs**, ce qui va générer une trop grande charge au niveau de la transmission sur le réseau.

Le **codec** G723 est éliminé également, car il existe d'autres **codecs** comparables mais open source comme Speex, iLBC et Opus, avec les deux modes LP (qui utilise le **codec** voix SILK) et Hybride (qui utilise les **codecs** SILK et CELT).

Après cette première comparaison, il ne subsiste que les **codecs** iLBC, Speex et Opus. A présent, nous allons effectuer une comparaison qui se base sur le nombre de paquets générés et la valeur de **BO** et **SO** (cf. Tableau 2.7).

Pour favoriser la transmission de la voix et diminuer le temps d'attente au niveau des files d'attente, nous avons décidé de tenter de ne transmettre qu'un seul paquet de voix dans chaque supertrame. Selon le tableau 2.6, par exemple, le **codec** iLBC génère un seul paquet de voix chaque 20 ms donc la valeur minimale de **BO** et **SO** est égale à 1 pour avoir au moins un paquet de données dans chaque supertrame. Supposons que nous ayons choisi d'utiliser $BO = SO = 2$, donc le **SD** est égal à 61,44 ms. On déduit que dans la période de **SD** le **codec** iLBC génère trois paquets de voix ; dans les pires cas, la taille de l'entête de la sous-couche MAC et la sous-couche physique ne dépasse

pas 45 octets et la taille d'un paquet de voix généré par le **codec** est égale à 34 octets alors que la taille d'un **LIFS** (*Long InterFrame Spacing*) est égale à $640 \mu s$; la taille maximale d'un paquet de voix à transmettre est donc égale à 79 octets et nécessite $7,59 ms + 3 \times 640 \mu s = 9,51 ms$: il faut donc réserver trois slots.

À partir des calculs effectués et comme la norme 802.15.4 définit une durée minimale pour la période **CFP** égale à 7,04 ms, le nombre maximal de nœuds qui peuvent transmettre des **GTS** ne dépasse pas 4 nœuds si on choisit de ne transmettre pas plus qu'un seul paquet de voix dans une supertrame. Par contre, nous pouvons avoir 6 nœuds qui transmettent la voix dans le cas d'une transmission d'un seul paquet par supertrame dans un seul sens.

De plus, si on transmet plusieurs paquets dans une supertrame, le temps d'attente au niveau de la file d'attente sera plus long. Par exemple, dans le cas de iLBC avec **BO** = **SO** = 2, le premier paquet doit attendre 51,93 ms (la durée nécessaire jusqu'à la période de **GTS** dans le pire des cas), le second paquet doit attendre $31,93 ms + 7,59$ (la durée d'attente jusqu'à l'arrivée du **GTS** + la durée nécessaire pour la transmission du premier paquet) et le troisième paquet doit attendre $11 ms + 7,59 ms$ dans le cas de transmission sans acquittement. Donc, la durée moyenne d'attente est égale à 36,68 ms contre 26,88 ms dans le cas de transmission d'un seul paquet par supertrame.

Le tableau 2.7 présente les valeurs de **BO** et **SO** qui correspondent à chaque type de **codec** et le taux d'utilisation (**TU**) qui représente le nombre de paquets transmis dans chaque supertrame. Les valeurs de **BO** et de **SO** ne dépassent pas la valeur 2, ce qui est expliqué dans le tableau 2.8 qui présente différentes valeurs de **SD**. À partir des calculs présentés dans le tableau 2.8, nous avons conclu que la valeur maximale de **BO** et **SO** ne doit pas être supérieure à 3, puisque la valeur maximale de la latence pour une transmission voix ne doit pas dépasser 150 ms [99].

Pour les **codecs** iLBC, Speex et Opus (avec des trames de taille de 2,5, 5, 20 et 40 ms), le pourcentage d'utilisation est supérieur à 1, ce qui permet d'avoir plusieurs paquets transmis dans une seule supertrame. Comme la durée de la supertrame est courte (cf. tableau 2.7), nous risquons d'avoir des rejets de paquets. Par exemple, si nous effectuons une communication audio en utilisant le **codec** iLBC qui génère un paquet de taille 20 ms et utilise **BO** = **SO** = 1 ; la transmission d'un paquet de voix nécessite 3,17 ms : il faut donc réserver deux slots par supertrame.

La réservation, dans la norme IEEE 802.15.4, s'effectue toujours à la fin de la supertrame. Le nœud doit alors attendre 26,88 ms à chaque supertrame avant de pouvoir transmettre le paquet. Comme le nombre de slots réservés pour la transmission est égal à 2, ce qui est équivalent à 3,84 ms (avec la durée d'un slot égale à 1,92 ms), le temps qui reste après la transmission ne permet pas de transmettre un autre paquet ($3,84 - 3,17 = 0,67 ms < 3,17 ms$), nous pouvons alors avoir une accumulation de paquets dans la file d'attente. Le **codec** génère 180 000 paquets dans une heure et le nombre de supertrames dans une heure est égal à 117188. Donc, le nombre de paquets qui ne peuvent pas être

Codec	Durée d'un paquet de voix (ms)	BO = SO	SD (ms)	TU
iLBC	20	1	30.72	1.53
	30			1.02
Speex	30	1	30.72	1.02
	34	2	61.44	2
Opus (mode LP)	10	0	15.36	0.30
	20	1	30.72	1.53
	40	2	61.44	1.47
	60	2	61.44	1.02
Opus (mode Hybride)	10	0	15.36	0.30
	20	1	30.72	1.53
Opus (mode MDCT)	1.5	0	15.36	6.15
	5	0	15.36	3.07
	10	0	15.36	0.30
	20	1	30.72	1.53

TABLE 2.7: Correspondance entre le codec et les valeurs de BO et SO

BO = SO	SD $\times 16 \times 10^{-3}$ (ms)
0	15.36
1	30.72
2	61.44
3	122.88
4	245.76

TABLE 2.8: Valeur de SD

transmis et qui seront en attente (perdus ou droppés) dans la file d'attente est égal à 62812 ($180000 - 117188 = 62812$ paquets).

Les paquets qui ne sont pas transmis ont une taille égale à 34 octets, la taille maximale d'une mémoire RAM pour un capteur est de l'ordre de 128 koctets [100] (cette valeur de RAM est rare sur un noeud 802.15.4), donc le nombre maximal de paquets que l'on peut garder dans une file d'attente est égal à 3764 paquets. Ainsi, le nombre de paquets qui seront rejetés est égal à 59048 paquets ou moins, car la RAM va servir à stocker d'autres choses, ce qui représente 32.82% du nombre total des paquets générés par le [codec](#) iLBC. Donc, lorsque le taux d'utilisation est très supérieur à 1, nous pouvons avoir un grand pourcentage de paquets rejetés.

À partir du tableau 2.7, nous pouvons déduire que les meilleurs [codecs](#) sont Opus avec un paquet chaque 60 ms, iLBC avec un paquet chaque 30 ms et Speex avec un paquet chaque 30 ms pour un taux d'utilisation égal à 1,02 (proche de 1).

À partir des résultats des tests effectués dans [101], les auteurs ont montré que le [codec](#) Opus avec un débit égal à 11 kbits/s est comparable à iLBC (qui utilise un débit égal à 15 kbits/s) et meilleur que Speex (qui utilise un débit égal à 11 kbits/s). De plus, ces travaux ont montré que le [codec](#) Opus avec des débits de 20 kbits/s et 30 kbits/s est meilleur que G719 (avec un débit de 32 kbits/s), et Speex (avec un débit de 24 kbits/s).

À l'issu de cette étude, notre choix se porte donc sur le [codec](#) Opus qui offre un débit raisonnable et une qualité de voix meilleure que les autres [codecs](#).

Après cette étude théorique, nous présentons une étude sur la transmission de la voix.

2.6.2 Etude de la transmission de la voix

Dans le projet *CANet*, la communication voix peut être initiée de deux façons. Le premier cas survient lorsque l'utilisateur de la canne appuie sur le bouton d'appel d'aide (figure 2.20). Le deuxième cas se présente lorsque le centre de contrôle reçoit un message d'urgence ou d'alerte (figure 2.21).

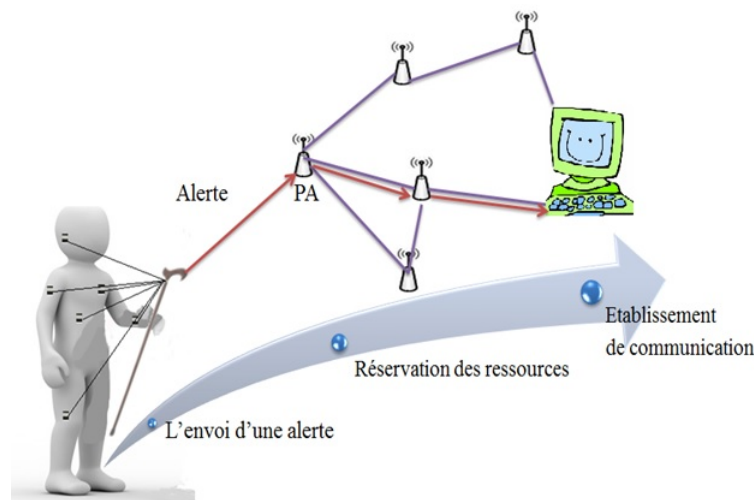


FIGURE 2.20: Appel d'urgence

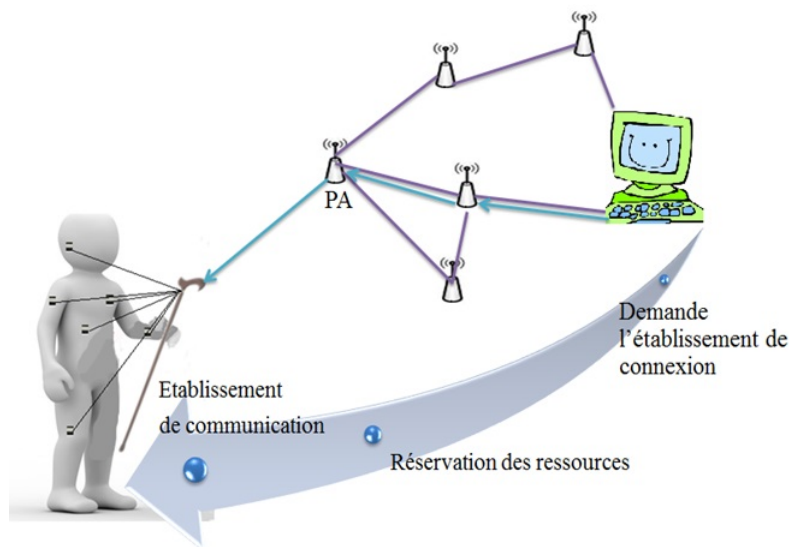


FIGURE 2.21: Réception d'un appel

Afin de bien étudier le cas de la transmission de la voix, nous fixons les hypothèses suivantes :

- **codec** utilisé : Opus
- débit : 30 kbit/s
- taille de la trame de données : 75 octets
- durée d'une trame : 20 ms

Si nous utilisons les paramètres **BO** = **SO** = 0, la **SD** sera égale à 15,36 ms avec **SD** = **BI**. La taille d'un slot est égale à 0,96 ms et la taille totale d'une trame de données **IEEE** 802.15.4 est égale à 632 bits (79 octets). À partir de ces informations, nous pouvons déduire le nombre de slots nécessaires pour la transmission d'une trame de données (**SNTD**).

$$SNTD = \frac{\frac{\text{Taille d'une trame de donnée} \times 1000}{250 \text{ kbits}}}{\text{taille d'un slot}} = \frac{\frac{632 \times 1000}{250000}}{0.96} = 3 \text{ slots} \quad (2.7)$$

Donc, pour transmettre une trame, si **BO** = **SO** = 0, nous utilisons 3 slots.

La taille minimale de la **CAP** est égale à 400 symboles, ce qui est équivalent à 6.4 ms. La taille d'un beacon dans le pire des cas est égale à 552 bits, c'est-à-dire une durée de 2.216 ms. La durée nécessaire pour la transmission du beacon et la période minimale de la CAP est égal à 8.616 ms ce qui est équivalent à 9 slots (La période CAP commence directement après l'émission de beacon). Donc, le nombre de slots libre est égal à 7 slots.

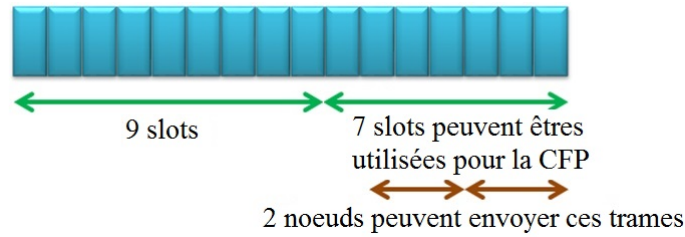


FIGURE 2.22: Supertrame utilisée pour le cas 1

Heureusement, nous pouvons supprimer et modifier la taille des champs de la trame beacon, comme le champ *Auxiliary Security Header*, *Pending Address fields* et le nombre de noeuds qui demandent des GTS. La taille du beacon peut passer de 552 bits à 320 bits (40 octets). La durée nécessaire de transmission d'un beacon devient 1.28 ms. Donc le nombre de slots nécessaires pour la transmission de beacon et la période minimale de **CAP** est de 8 slots, ce qui nous permet d'avoir 8 slots libres pour la **CFP**.

Si on réduit le nombre de noeuds à 2, la taille maximale du beacon devient égale à 200 bits (25 octets), ce qui correspond à 0.8 ms. Donc, 8 slots sont nécessaires pour la période **CAP** et il reste 8 slots pour la période **CFP**. De même, si nous n'avons qu'un seul noeud, la taille du beacon devient égale à 176 bits (22 octets). Donc, le nombre de slots nécessaires pour la période **CAP** est de 8 slots. Il reste 8 slots pour la période **CFP**.

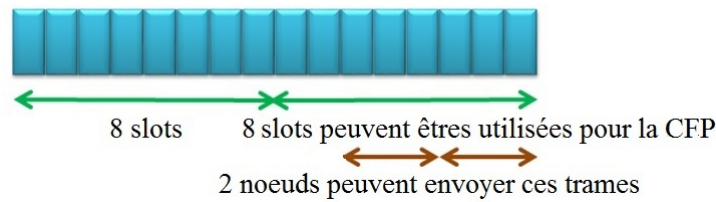


FIGURE 2.23: Supertrame utilisée pour le cas 2

Le tableau 2.9 présente le nombre de nœuds qui peuvent transmettre (Tx) et recevoir (Rx) des communications audio avec l'utilisation des différentes valeurs de BO et SO. Le tableau contient aussi le nombre de slots inutilisés et la perte de temps au niveau des slots utilisés.

BO = SO	Nb. nœuds	Nb. slots Tx	Nb. slots Rx	Nb. slots inutilisés	Temps perdu (ms)
1	2	2	2	3	2.62
2	3	2	2	1	5.24
3	3	2	2	2	10.26
4	3	2	2	2	20.96
5	3	2	2	3	41.92

TABLE 2.9: Information sur l'influence de la valeur de BO et SO

À partir de ce tableau, nous pouvons déduire que le nombre maximal de nœuds qui peuvent transmettre des communications audio dans la même supertrame est égal à 3 pour les valeurs de BO et SO de 2 et 3, avec la possibilité d'avoir 1 ou 2 slots qui ne sont pas utilisés.

L'importance de la latence pour la voix nous conduit à l'évaluer. Le tableau 2.10 nous permet de connaître la durée de la latence pour chaque valeur de BO et SO. La valeur acceptable de la latence définie pour la transmission de voix est entre 0 et 150 ms. Dans le tableau 2.10, les valeurs acceptables sont colorées en vert. Les valeurs qui sont acceptables mais très proches de la limite (150 ms) sont en jaune et les valeurs à éviter sont en rouge.

BO = SO	Nb. nœuds	Nb. slots inutilisés	Temps perdu (ms)	Latence (ms)
1	2	3	2.62	33.34
2	3	1	5.24	66.68
3	3	2	10.26	133.14
4	3	2	20.96	266.72
5	3	3	41.92	533.44

TABLE 2.10: Les valeurs acceptables de BO et SO

Pour BO = SO = 1 et 2, la valeur de la latence est acceptable, mais le temps perdu varie entre 2 et 5 ms. Dans le cas où BO = SO = 1, 2 slots ne seront pas utilisés. Par contre, pour BO = SO = 2, un seul slot ne sera pas utilisé. Nous préférons donc utiliser BO =

$SO = 2$ pour la transmission de la voix en délaissant $BO = SO = 1$ puisque ceci nous permet d'utiliser le maximum de slots de temps et permet à 3 nœuds de transmettre de la voix plutôt que 2 nœuds uniquement pour $BO = SO = 1$. La durée très courte de la supertrame pour $BO = SO = 2$ augmente la consommation de l'énergie, ce qui diminue la durée de vie de la canne. La consommation d'énergie dépend énormément de la période d'inactivité, et des modes de transmission et de réception. Les nœuds utilisent plus d'énergie lors de la réception que lors de la transmission. Dans notre cas $BO = SO$, donc il n'existe pas de période d'inactivité. Mais dans notre configuration nous utilisons la période CFP ce qui signifie que les nœuds ne peuvent transmettre des trames que dans les périodes dédiées et ils passent le reste du temps dans l'état *sleep*. Du coup, si nous choisissons d'utiliser la valeur 2 pour BO et SO , chaque nœud doit se réveiller chaque 61,44 ms ce qui ne permet pas de gagner au niveau de consommation d'énergie. Aussi, la taille de slot est petite ce qui signifie que le nœud passe plus de temps dans le changement de son état que dans le mode *sleep*. Par contre si nous choisissons les valeurs 3 pour BO et SO , chaque nœud dans le réseau doit se réveiller chaque 122,88 ms ce qui représente le double par rapport à $BO = SO = 2$. Aussi la durée de slot est plus grande ce qui nous permet d'avoir plus de temps d'inactivité (Dans le tableau 2.9, le temps perdu dans la période CFP est égal à 10,26 ms pour $BO = SO = 3$ et à 2,62 ms pour $BO = SO = 5$, 24 ms. Ce temps sera utilisé comme une période d'inactivité partagée entre les différents nœuds du réseau). Aussi le débit possible pour $BO = SO = 1$ et 2, inférieur à 35 kbit/s, est très faible. Avec un débit aussi faible la canne ne peut pas transmettre tous les messages nécessaires avec la communication vocale.

Il existe des périodes où la canne n'envoie pas des trames dans les GTS réservés, ce qui représente une perte de temps. Pour cette raison, nous préférons utiliser $BO = SO = 3$ afin de s'assurer que nous utilisons toutes les périodes réservées.

2.6.3 Algorithme de gestion de la transmission audio

Lors de la réception d'une demande de transmission audio, le $CMAF$ commence par préparer les paramètres de transmission dédiés à la voix. Il recalcule la taille des slots selon les nouvelles valeurs de BO et SO . Ensuite, il vérifie si le nombre de GTS réservés est égal à 7. Si c'est le cas, il procède à l'annulation de certaines réservations afin de satisfaire le nœud demandeur de la transmission de la voix. Si le nombre de GTS est inférieur à 7, alors il vérifie si la taille minimale de la CAP est respectée. Si la taille n'est pas respectée, il procède alors à l'annulation des réservations. Sinon, il effectue la réservation et vérifie de nouveau la condition. Finalement, le $CMAF$ met à jour sa table de réservation de GTS et transmet le beacon avec les nouveaux paramètres de réservation : BO et SO .

Nous avons également envisagé d'autres pistes pour rendre les valeurs de BO et SO plus dynamiques, comme par exemple : (i) en faisant changer les valeurs associées de BO et SO en fonction du nombre de nœuds dans le réseau ; (ii) ou en faisant changer les valeurs

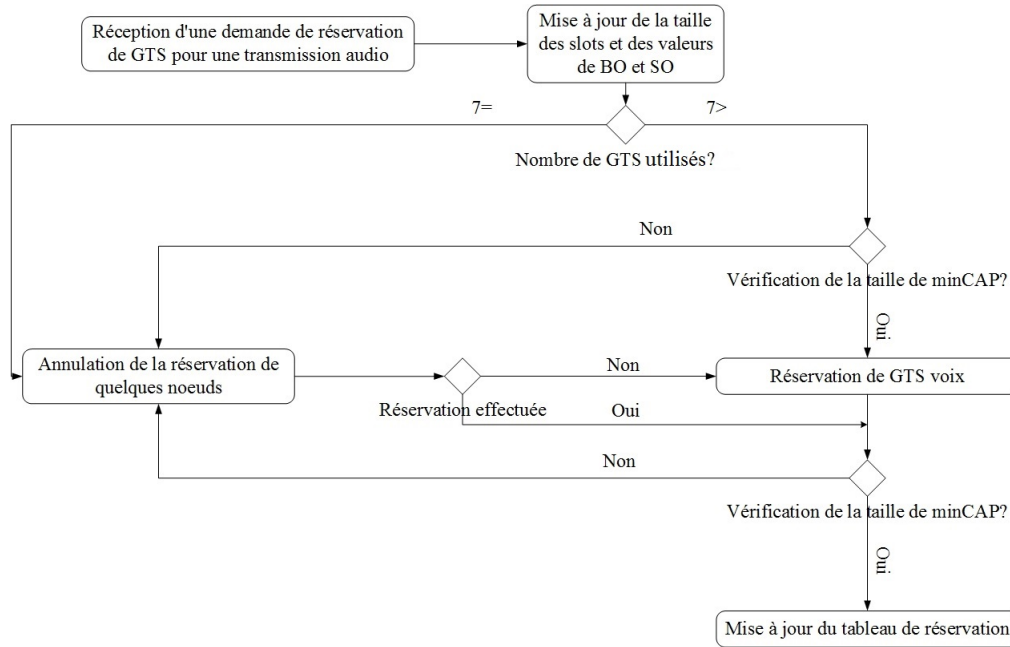


FIGURE 2.24: Réserve des ressources pour la transmission audio

de BO et SO en fonction du temps de latence et du nombre de nœuds demandeurs d'une communication voix.

2.6.4 Expérimentations

Après l'étude théorique effectuée sur une grande variété de [codecs](#), présentée en 2.6.1 [P5], nous présentons dans cette section, une simulation de différents [codecs](#) évalués et testés comparativement. Nous avons modélisé et simulé sous OMNet++ ces transmissions de la voix. La Figure 2.25 représente les étapes de transmission d'un fichier de voix entre deux nœuds (un coordinateur et un nœud normal) [P5].

L'application dans le nœud normal lit le fichier audio mp3. Elle utilise ensuite un des [codecs](#) préinstallés sur l'ordinateur. Finalement, l'application prépare des messages de voix qui ont des caractéristiques conformes à celles de la norme 802.15.4. Les couches MAC et PHY sont les responsables de la transmission des paquets audio qui seront reçus et traités par la couche applicative du coordinateur.

Suite à la réception des messages audio, la couche application du coordinateur va recréer petit à petit le fichier total transmis par la couche applicative du nœud émetteur initial.

Les premiers tests que nous avons effectués avaient pour but de valider la modélisation développée pour la simulation. Nous avons utilisé le [codec](#) Speex avec un message de 30 ms et un débit de 24,6 kbit/s, ce premier test a montré qu'il y avait une légère modification au niveau fichier de réception qui est audible et gênante (cf. Figure 2.26) [P5].

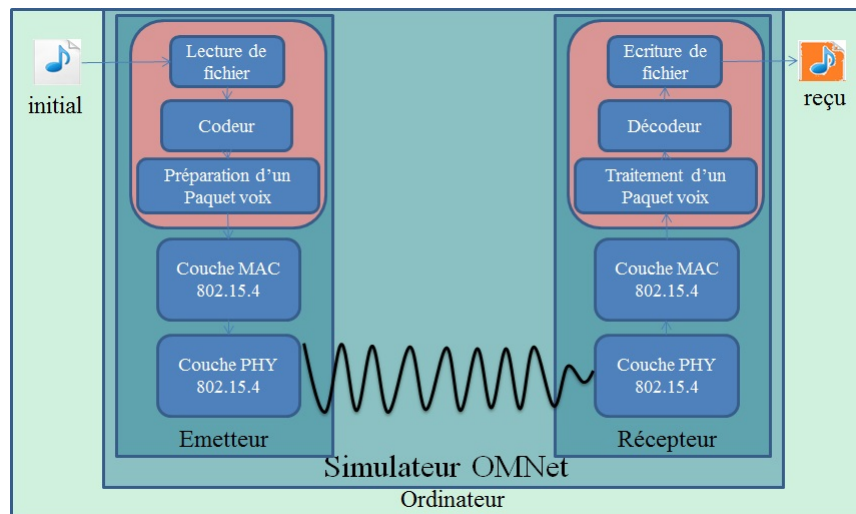


FIGURE 2.25: Etapes de transmission de voix

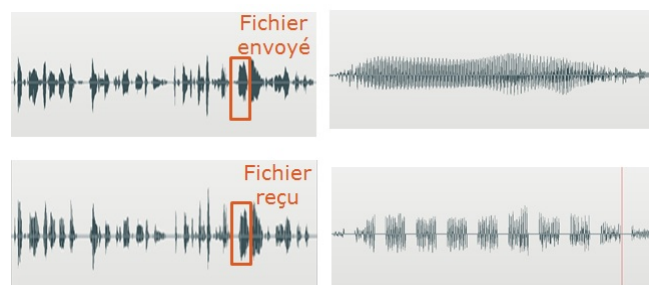


FIGURE 2.26: Transmission avec l'utilisation de codec Speex

Nous avons enfin testé l'effet du codage et du décodage d'un fichier voix en utilisant le [codec](#) Opus (cf. Figure 2.27) [P5].



FIGURE 2.27: Résultat du codec Opus avec un débit de 24.6 kbits/s

Lorsque nous écoutons les sons résultants, nous remarquons qu'avec l'utilisation de [codec](#) opus, il existe une faible dégradation de la qualité de son. L'audio régénéré par l'Opus est très proche du son original. Par contre, nous remarquons une forte dégradation de son avec le [codec](#) Speex (cf. Figure 2.26).

D'après les résultats de ces simulations, nous recommandons donc d'utiliser le [codec](#) Opus pour les communications de type voix. Les comparaisons sont basées essentiellement sur la qualité subjective de la voix sans prendre en considération la consommation énergétique.

2.7 Conclusion

Dans ce chapitre, nous avons commencé par analyser les profils des capteurs en étudiant les différents capteurs qui peuvent être utilisés dans le projet *CANet*. Nous avons ensuite proposé des critères de classification. Nous avons classifié les capteurs en 8 profils et nous avons créé 2 profils abstraits qui peuvent être utilisés par les capteurs dans les cas d'urgence ou d'alerte. Après cette étude, nous avons présenté la topologie globale proposée avec les technologies associées. Puis, nous avons présenté notre couche de différenciation et nous avons détaillé son fonctionnement.

Afin de terminer l'analyse des profils, nous avons effectué une étude qui se base sur la topologie étoile et le mode avec beacon de la norme [IEEE 802.15.4](#). Cette étude nous a permis de compléter le tableau de profils avec les différentes valeurs de [BO](#) et [SO](#) adéquates. Finalement, nous avons présenté une étude sur la transmission de la voix. Dans cette étude, nous avons choisi le [codec](#) adéquat à notre solution et nous avons associé les valeurs de [BO](#) et [SO](#) à ce type de trafic.

Dans le chapitre suivant, nous présenterons les simulations et les analyses de performances que nous avons effectuées.

Chapitre 3

Evaluation des performances et modélisation

Dans les deux premiers chapitres, nous avons introduit les principaux problèmes de l'*e-santé* et les solutions proposées. Parmi ces solutions, nous avons proposé l'intégration d'une nouvelle couche de communication dans le projet *CANet*. Cette couche a comme rôle la gestion des différents types de trafics générés par les capteurs de la canne et le maintien de la synchronisation entre les périodes de transmission et le type de la trame à transmettre.

Dans ce chapitre, nous allons évaluer et tester par simulation nos propositions. Nous présenterons l'analyse dans le cas de la présence de deux profils différents. Cette étape détaille la comparaison des performances de l'empilement protocolaire, dans le respect de la norme, avec et sans couche de différenciation. Nous évaluerons ensuite les performances du réseau dans le cas de la présence d'une alerte. Dans ce cas-là, nous testerons essentiellement l'efficacité de l'adaptation de la couche de différenciation aux variations internes des applications.

Finalement, nous effectuerons des simulations qui modélisent des trafics temps réels pour la transmission de la voix.

3.1 Choix du simulateur

OMNet++ (Objective Modular Network Test bed in C++)[\[102\]](#) est un simulateur multiplateforme à événements discrets développé en C++ pour la modélisation des communications dans un réseau, pour les architectures multiprocesseur et les systèmes parallèles ou distribués [\[103\]](#). OMNet est assez populaire dans la communauté scientifique aussi bien que dans la communauté industrielle. Il n'est pas un simulateur en lui-même mais nous pouvons le considérer comme un compilateur des plateformes de simulation comme INET [\[104\]](#), INETMANET [\[105\]](#), etc. Il se présente comme un ensemble de modules

interconnectés et hiérarchisés d'une manière à les rendre extensibles et réutilisables. La communication s'effectue à travers l'échange des messages via des portes. Les liens entre les portes permettent la configuration de délais de propagation et de taux d'erreur. La définition des différents protocoles, couches et liens, s'effectue dans le fichier de description de réseau (un fichier à l'extension .ned). Il contient un outil graphique qui permet également de définir des topologies et de visualiser les transferts des trames sur le réseau.

Dans [106], les auteurs présentent une comparaison entre OMNet++ et NS2 principalement. Ils ont montré qu'OMNet++ offre une très bonne base pour la simulation des RCSF. De plus, OMNet++ offre de meilleures performances que celles de NS2. Les auteurs ont mentionné qu'OMNet++ est légèrement meilleur qu'OPNET. OMNet++ surpasse NS2 et NS3 avec la taille de la communauté scientifique et industrielle qui l'utilisent. Il n'est pas un simulateur dédié à un seul type de réseau, il a la capacité d'intégrer plusieurs technologies et de modéliser n'importe quel algorithme.

OMNet++ est assez comparable au simulateur OPNET mais il est open source, ce qui donne un très grand avantage à ce simulateur pour les scientifiques et centres de recherches. D'autre part, OMNet++ peut intégrer la modélisation des protocoles des autres simulateurs. Des développeurs offrent un outil d'importation qui permet d'effectuer les modifications nécessaires automatiquement. Cette option a enrichi énormément les différentes plateformes d'OMNet++.

3.2 Validation des valeurs de BO et SO

Dans le chapitre 2, nous avons présenté une étude théorique sur l'influence de la variation de BO et SO sur les performances du réseau. Cette étude nous a permis de compléter le tableau des profils par les valeurs de BO et SO les plus adéquates à chaque profil (cf. tableau 2.5 du chapitre 2).

Dans cette section, nous présentons une simulation de la transmission des trames dans les périodes CFP et CAP de la norme 802.15.4 avec différentes valeurs de BO et SO. Cette étude pratique nous aide à valider l'étude théorique et vérifier si les valeurs choisies sont optimales ou non.

Nous avons effectué des simulations pour deux scénarii avec différentes valeurs de BO et SO et un nombre de nœuds variable. Notre réseau simulé contient un seul coordinateur et le nombre de nœud feuilles RFD varie entre 1 et 10. La topologie étoile est utilisée. Les valeurs de BO et SO varient entre 0 et 14. Le temps d'inter-arrivée des messages est égal à 30ms ou 60s. La taille de payload générée par l'application est égale à 10 ou 70 octets.

Dans le premier scénario, nous observons l'influence de la variation de BO et SO sur le nombre de messages transmis pour les nœuds qui sont configurés selon les paramètres présentés dans le tableau 3.1. Le nombre de slots réservés par un nœud dépend de

la taille du premier message transmis. Les slots réservés dans la période CFP sont maintenus jusqu'à la fin de la simulation.

Paramètres	Valeurs
Durée d'inter-arrivée des messages	30ms
BO = SO	0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13 et 14
Nombre des nœuds	1 et 5 nœuds RFD et 1 coordinateur
Durée de la simulation	1 heure
Taille de la payload	70 octets
Taille du buffer	10 trames
Mode de transmission	GTS

TABLE 3.1: Paramètres utilisés dans le premier scénario

La figure 3.1 présente le nombre de messages reçus dans la période CFP. Nous remarquons que le nombre de messages reçus diminue avec l'augmentation de la valeur de BO et SO. Le nombre maximal de messages reçus est pour BO = SO = 0 avec l'existence d'un seul nœud dans le réseau. Dans le cas de l'existence de plusieurs nœuds dans le réseau, le nombre maximal de messages reçus est pour BO = SO = 1 dans le cas de l'utilisation de 10 nœuds. Le nombre de messages reçus a augmenté dans le cas de BO = SO = 1 pour 10 nœuds parce que les nœuds ont plus de temps pour transmettre leurs messages puisque la taille des slots réservés a augmenté. Le nombre des slots réservés par chaque nœud a donc diminué alors les nœuds qui n'ont pas pu avoir des slots GTS dans le cas de BO = SO = 0 ont pu ainsi obtenir des slots.

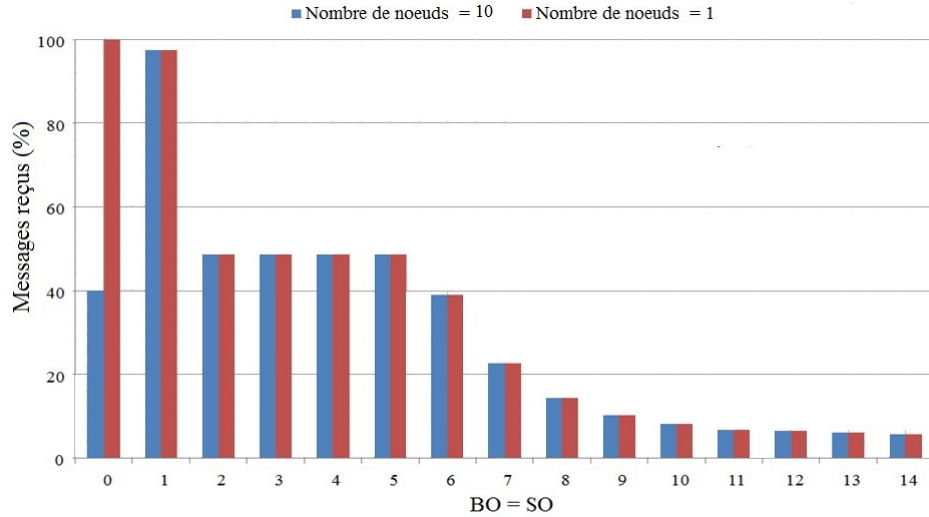


FIGURE 3.1: Pourcentage des messages reçus dans CFP avec BO = SO

La figure 3.2 illustre l'évolution du nombre de slots réservés par chaque nœud. Pour BO = SO = 0, le nombre de slots nécessaires pour la transmission des données est égal à 4 slots pour chaque nœud. Ici, seuls deux nœuds peuvent transmettre leurs messages. A l'inverse, lorsque BO = SO = 1, la durée du slots devient plus grande. Du coup, le nombre de slots nécessaires pour la transmission des données pour chaque nœud et pour le minCAP (représente la période minimale fixée par la norme pour la période CAP) a

diminué de 2 slots. Les slots inutilisés seront réservés pour les autres nœuds (figure 3.2 (a) et (b)).

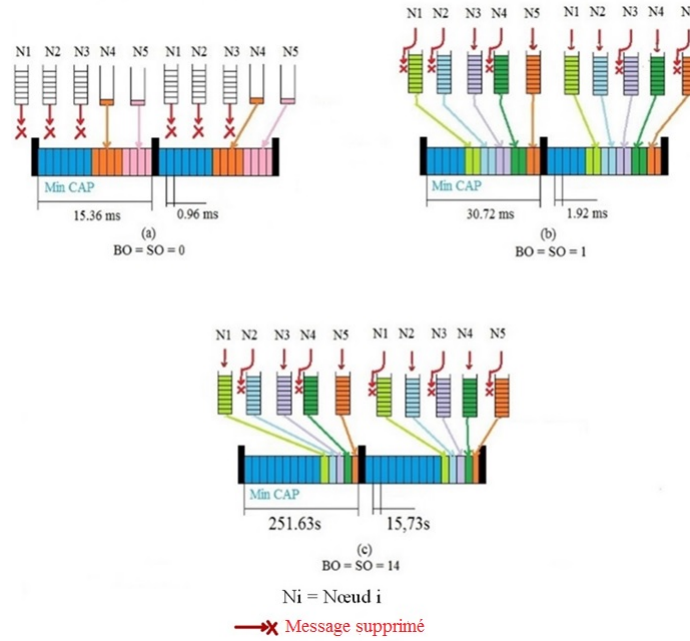


FIGURE 3.2: Transmission des messages pour $BO = SO = 0, 1$ et 14

Si la SD augmente, la durée d'attente du début de la période de transmission suivante augmente pour chaque nœud. Par exemple, si $BO = SO = 14$, SD est égal à 251,66s. Donc, les nœuds doivent attendre 251,66s entre deux périodes de transmission successives (figure 3.2 (c) et figure 3.3). Au début de la supertrame, les nœuds ont généré 8367 messages, seuls les 10 premières trames seront stockées dans la file d'attente et 8357 seront perdues car rejetées. Pour ces raisons, le nombre de messages transmis diminue lorsque SD augmente.

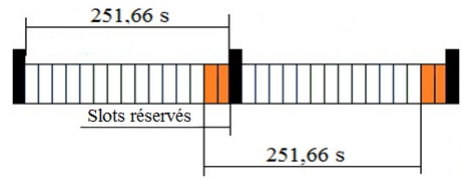


FIGURE 3.3: Période de transmission pour $BO = SO = 14$

Nous remarquons dans la figure 3.1 que pour $BO = SO = 2, 3, 4$ et 5 , le même nombre de messages est transmis. La durée de SD pour ces valeurs est de 61,44ms, 122,88ms, 245,76ms et 491,52ms successivement. Dans une seule supertrame, le nœud génère 1, 4, 8 et 16 messages et la durée d'un slot est égale à 3,84 ms, 7,68 ms, 15,36 ms et 30,72 ms successivement pour $BO = SO = 2, 3, 4$ et 5 . Pour ces valeurs de BO et SO , les nœuds peuvent seulement transmettre la moitié des messages générés. Après une certaine durée, le tampon sera rempli et il n'acceptera plus de nouveaux messages. Finalement, les valeurs optimales sont $BO = SO = 0$ pour un seul nœud et $BO = SO = 1$ pour 5 nœuds. Dans la deuxième simulation, nous avons changé les paramètres par

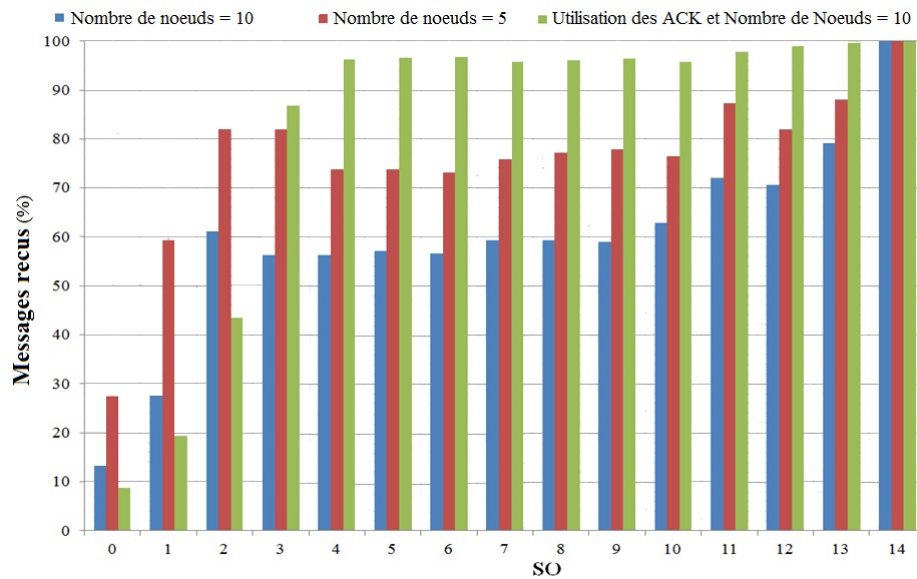
ceux donnés dans le tableau 3.2 afin de les adapter aux caractéristiques de la première classe.

Paramètres	Valeurs
Durée d'inter-arrivée des messages	60ms
BO	0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13 et 14
SO	0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13 et 14
Nombre des nœuds	5 et 10 nœuds feuilles et 1 coordinateur
Durée de la simulation	1 heure
Taille de la payload	10 octets
Taille du buffer	10 trames

TABLE 3.2: Paramètres de la deuxième simulation

Avec cette configuration, si $BO = SO$, le nombre de messages reçus est égal à 100% des messages émis. La variation de la valeur de BO et SO n'a pas une grande influence puisque le trafic généré n'est pas lourd.

Dans cette classe, les capteurs ont un message à transmettre toutes les 60 ms. Pour cette raison, l'utilisation d'une petite valeur de BO et SO n'est pas la bonne solution. Si nous utilisons une grande valeur de BO et SO , nous pouvons augmenter la durée de la période inactive, ce qui permet de diminuer la consommation d'énergie des nœuds du réseau. Un équilibre entre la durée maximale de SD et la durée maximale de la période inactive doit être identifié afin de trouver un compromis entre le nombre de messages bien reçus et la conservation d'énergie.

FIGURE 3.4: Pourcentage des messages reçus dans la CAP avec $BO = 14$

On voit dans la figure 3.4, que le nombre de messages transmis avec succès sans demande d'un ACK pour $SO = 2$ est plus grand que celui avec demande d'ACK. Cela est dû au temps d'attente de l'ACK par le nœud source de la trame. Si le nœud ne reçoit pas l'ACK avant la fin de la durée d'attente de son chien de garde, il considère la trame

comme perdue et il procède à la retransmission de cette dernière. Dans ce cas, le même message est envoyé au moins 2 fois. Puisque la durée de **SD** n'est pas assez longue, le nœud ne peut pas retransmettre l'ancien message et commence la transmission d'un nouveau dans la même période **SD**. Dans le cas où les **ACK** sont désactivés, les nœuds transmettent leurs messages sans attendre l'**ACK**.

A partir de **SO** = 3, le nombre de messages reçus avec succès avec l'utilisation de l'**ACK** est plus grand que le cas sans **ACK**. Cela peut être expliqué par la longueur de la période **SD** qui est devenue plus importante, ce qui diminue le nombre de collisions et offre au nœud plus de temps pour retransmettre l'ancienne trame et en transmettre de nouvelles.

Si la durée de **SD** augmente, les nœuds ont plus de chance de transmettre leurs messages. De plus, si le nombre de nœuds augmente, le nombre de messages transmis avec succès diminue parce que le nombre de nœuds qui ont tenté d'accéder au médium a augmenté, ce qui fait croître le nombre de collisions dans le réseau. Pour cela, si le nombre de nœuds augmente, la durée de **SD** doit augmenter également ; la valeur de **SO** doit augmenter aussi.

Dans notre étude théorique, nous avons fixé les valeurs minimales de **SO** à 7 pour s'assurer que nous avons une durée minimum qui contient les périodes active et inactive. Notre but était de trouver les valeurs optimales de **BO** et **SO** qui permettent d'augmenter le nombre de messages reçus avec succès et en même temps, optimiser la consommation de l'énergie. Après nos simulations, nous pouvons déduire que l'intervalle [7, 14] contient les valeurs qui peuvent être utilisées pour les applications qui exigent la réception des trames.

Finalement, nous n'avons pas simulé la classe qui permet la transmission des données dans la période **CAP** et **CFP** en même temps pour deux raisons. Premièrement, les données de cette classe ne sont pas transmises périodiquement. Donc, le trafic généré n'a pas de grandes influences prédictibles sur les performances du réseau. Deuxièmement, dans le projet *CANet*, un seul nœud peut activer l'état d'urgence.

Dans cette section, nous avons présenté les résultats de notre modélisation et simulation de la transmission de messages dans les périodes **CAP** et **CFP**. Notre réseau est configuré avec des paramètres de deux types d'applications qui appartiennent à deux classes différentes qui utilisent l'une des deux périodes **CAP** ou **CFP**. Les valeurs de **BO** et **SO** trouvées dans l'étude théorique ont été vérifiées par simulation.

3.3 Etude par simulation de la couche de différenciation

Dans cette section, nous présentons les résultats de simulation effectués dans le cas de l'utilisation de la couche de différenciation et sans elle. Dans ces simulations, nous utilisons pour les applications des paramètres réels. Les informations générées par les capteurs sont transmises dans les périodes **CAP** et **CFP** adéquates et chaque canne est capable d'utiliser ces deux périodes dans la même supertrame.

3.3.1 Configuration réseau

3.3.1.1 Calcul du nombre de slots nécessaires pour la transmission

Lors de la demande d'un **GTS** dans la période **CFP**, la canne qui demande doit envoyer une requête qui contient le nombre de slots nécessaires pour sa transmission. Le nombre de slots nécessaires est calculé par l'équation 3.1.

$$NSR = \lceil \frac{DT + D_SIFS}{DS} \rceil \quad (3.1)$$

Avec :

- $NSR = \text{Nombre de Slots Réservés}$
- $DT = \text{Durée de transmission d'une trame} = TTM \times DTO \mu s$
- $DS = \text{La durée d'un slot} = \frac{SD}{16} s$
- $D_SIFS = 192 \mu s$
- $TTM = \text{Taille totale de la trame au niveau MAC (octet)}$
- $DTO = \text{Durée de transmission d'un octet} = 32 \mu s$

La valeur de NSR obtenue par l'équation (3.1) sera transmise au coordinateur afin d'effectuer la réservation des slots nécessaires.

3.3.1.2 Calcul de la valeur BO et SO

Dans le chapitre 2, nous avons présenté la topologie qui sera utilisée avec notre solution. Nous avons associé à chaque profil de capteurs, l'intervalle des valeurs de **BO** et **SO** les plus adéquates à ces caractéristiques.

Dans chaque profil, nous retrouvons différents capteurs qui ont des fréquences de génération de messages différentes, ce qui rend la **SD** importante et utile, en particulier pour les capteurs qui ont une fréquence plus élevée que les autres.

Pour cette raison, le coordinateur choisit la valeur de **BO** et **SO** en fonction de l'application la plus rapide dans la génération des messages.

Dans notre étude, nous ne prenons pas en considération la période d'association des cannes à un coordinateur (**CMAF**). Mais l'échange des messages définis par la norme dans cette période peut être utilisé pour informer le **CMAF** par les applications utilisées. Les informations qui doivent être envoyées vers le **CMAF** sont : le débit, la fréquence de génération des messages et la période de transmission. Le coordinateur ne s'intéresse ici

qu'aux applications qui utilisent la période **CFP**. Ces informations seront enregistrées dans la table des services de la couche Management. Cette table permet à la couche Management de choisir les bonnes valeurs de **BO** et **SO** qui doivent être utilisées.

Le coordinateur calcule la valeur de **SO** à l'aide de l'équation (3.2).

$$SO \leq \log_2(DIG) + \log_2\left(\frac{10^6}{960 * 16}\right) = \log_2(DIG) + 6,0247 = X \quad (3.2)$$

Avec :

$$\begin{cases} Si X \geq \lfloor X \rfloor + 0.5 \text{ alors } SO = \lceil X \rceil \\ Si X \leq \lfloor X \rfloor + 0.5 \text{ alors } SO = \lfloor X \rfloor \end{cases}$$

Et DIG = Durée Inter-Génération des messages

Le calcul de **BO** est fait par l'équation (3.3). Cette équation est identique à celle de **SO** dans le cas de la transmission de voix seulement, puisque nous avons une durée maximale de latence qui doit être respectée. S'il n'existe pas une communication vocale dans le réseau, le coordinateur essaye de maximiser la durée de période inactive avec la prise en considération des conditions liées aux trames transmises dans la période **CFP**.

$$BO < \log_2(TF \times DIG) + 6.0247 \quad (3.3)$$

Donc :

$$BO = \lfloor \log_2(TF \times DIG) + 6.0247 \rfloor - 1 \quad (3.4)$$

Avec :

- $TF = \text{Taille de la File d'attente}$
- $D_LIFS = 640 \mu s$

La durée de **LIFS** sera utilisée à la place de la durée du **SIFS** si la taille de la trame dépasse 18 Octets (définie par la norme). Avec les équations (3.2) et (3.4), le coordinateur peut adapter la durée de **SD** et de la période inactive selon les besoins des applications les plus exigeantes. Les calculs sont effectués essentiellement pour assurer la transmission des trames dans la période de **GTS** sans perte, puisque leurs informations sont importantes et précieuses.

3.3.2 Transmission dans les deux périodes de la même supertrame

La norme IEEE 802.15.4 n'offre pas une solution pour la transmission des trames dans les périodes **CAP** et **CFP** de la même supertrame. L'algorithme de **CSMA/CA** utilisé

dans le mode beacon est conçu d'une manière qui rend l'utilisation de deux périodes CAP et CFP par la même couche MAC pour deux trames différentes impossible.

Dans cette partie, nous proposons une solution qui se base sur les fonctions offertes par 802.15.4 afin de rendre l'utilisation simultanées des périodes CAP et CFP de la même supertrame possible.

3.3.2.1 Paramètres de simulation

Paramètres		Valeurs
Topologie		étoile
Nombre de nœuds		2, 3, 6, 8 (incluant le Coordinateur)
Type de Trafics		Capteur de rythme cardiaque échantillonné et capteur de type accéléromètre
Sens de transmission des données		Vers le coordinateur
Taille de file d'attentes au niveau de la couche Management		20 trames
Gestion des acquittements	CSMA/CA (CAP)	Avec ACK
	GTS (CFP)	Avec ou sans ACK

TABLE 3.3: Paramètres des simulations

Le tableau 3.3 présente les paramètres de configuration que nous avons utilisés dans ces simulations. La topologie utilisée est l'étoile. Il existe donc un seul coordinateur, et N nœuds feuilles dans le réseau qui sont connectées à ce dernier. On considère un seul domaine de collision. Les trames transmises dans la période CFP peuvent être acquittées ou non acquittées.

Le nombre de nœuds est égal à 2, 3, 6 puis 8 en incluant le coordinateur. Chaque nœud contient deux applications qui génèrent deux types de trafics. Ces trafics représentent les informations d'un capteur de rythme cardiaque (APP1) et celles d'un capteur de type accéléromètre (APP2). Les messages générés par les applications sont envoyés vers le coordinateur.

Les messages générés par l'APP1 ont une priorité plus faible que les messages générés par l'APP2. Les messages de l'APP1 sont donc envoyés dans la CAP et les messages de l'APP2 dans la CFP qui nécessite, elle, une réservation du nombre de slots nécessaires pour la transmission.

Dans la période CFP, les émetteurs des messages peuvent demander ou pas au coordinateur d'acquitter les messages bien reçus. Pour cette raison, nous allons tester l'influence de la présence d'acquiescement dans la CFP.

3.3.2.2 Transmission dans l'une des deux périodes

Deux scénarios sont possibles dans le cas de la transmission dans une seule période CAP ou CFP :

- dans le premier scénario, nous transmettons des données dans la période CAP uniquement, en effectuant une réservation des GTS dans la période CFP. Notre objectif est de tester l'influence du débit de données sur le réseau, dans les périodes CFP, avec la présence de réservation des GTS sans avoir des données transmises,
- dans le second scénario, nous transmettons des données dans la période CFP sans avoir de trafic dans la période CAP, avec l'existence de réservation des slots GTS. On réserve donc les slots nécessaires pour la transmission pour chaque nœud sans les utiliser.

Les messages générés par les applications APP1 et APP2 n'ont pas les mêmes priorités et ils ne sont pas transmis dans les mêmes périodes. Les messages générés par l'APP1 ont une priorité faible. Ils sont transmis dans la période CAP. Par contre, les messages générés par l'APP2 ont une priorité moyenne, ils sont transmis dans la période CFP.

Tous les nœuds dans le réseau réservent des GTS pour la transmission des trames avec une priorité moyenne. Les nœuds dans le réseau utilisent les mêmes applications avec les mêmes configurations. Pour effectuer les simulations, nous avons choisi d'utiliser une application qui simule le capteur de rythme cardiaque échantillonné (tableau 3.4). La configuration de simulation est présentée dans le tableau 3.3.

Type de capteur	Inter-messages	Taille de message
Capteur de rythme cardiaque échantillonné	20 ms	3 Octets

TABLE 3.4: Paramètres des simulations

Le débit généré par cette application est égal à 1200 bits/s, ce qui est très inférieur au débit maximal théorique de 802.15.4 (250 Kbit/s).

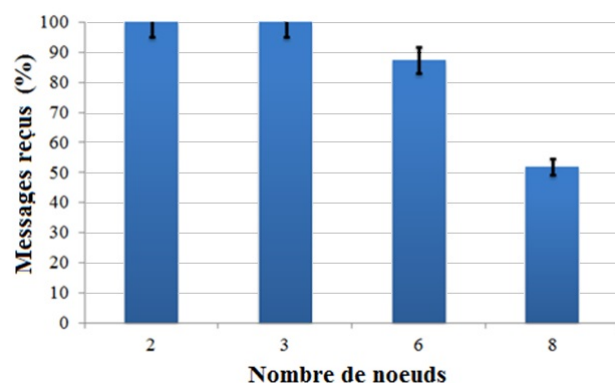


FIGURE 3.5: Pourcentage des messages reçus

La figure 3.5 présente le pourcentage des messages reçus dans la période CAP. Pour un petit nombre de nœuds émetteurs (1 et 2), le coordinateur reçoit tous les messages envoyés par ces nœuds. Par contre, pour un plus grand nombre de nœuds, le coordinateur reçoit 90% et 55% des messages pour 5 et 7 nœuds respectivement. Cette diminution est due à l'augmentation du temps d'attente pour accéder au canal et au nombre d'essais de retransmission effectués avant de réussir finalement ou d'échouer pour cette émission. Ceci augmente considérablement le nombre de trames perdues à cause du débordement des files d'attentes (voir figure 3.6) et du nombre d'échecs de transmission (voir figure 3.7).

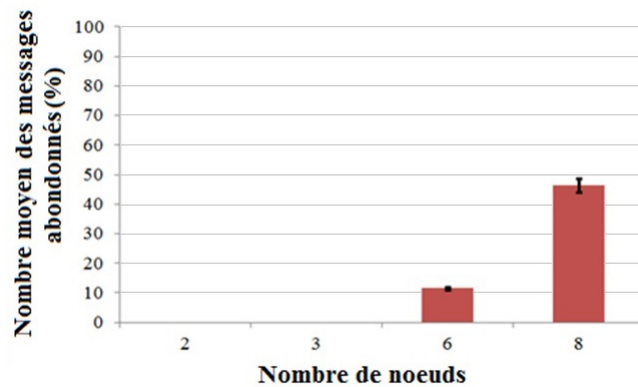


FIGURE 3.6: Nombre de messages non entrés dans la file FMT (avec conservation des trames qui seront transmises en CSMA/CA)

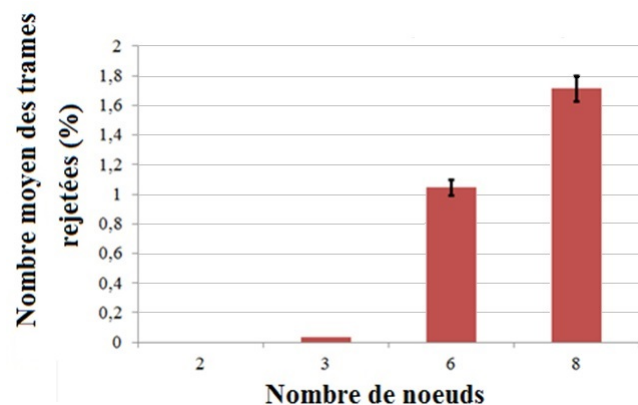


FIGURE 3.7: Nombre moyen de trames rejetées par la couche MAC après un échec de transmission)

Pour les résultats de transmission dans la période CFP, tous les messages sont bien transmis et le pourcentage de réussite est égal à 100%. Ce résultat est attendu puisque la réservation des slots dans la période GTS donne l'avantage aux nœuds pour transmettre leurs trames sans avoir de concurrence pour accéder au canal. De plus, la file d'attente ne déborde pas, ce qui signifie que tous les messages entrent dans la file FMT.

3.3.3 Transmission dans les deux périodes CFP et CAP de la même supertrame

Dans ce scénario, nous approchons du cas du projet *CANet* par l'utilisation d'une seconde application qui simule l'accéléromètre de la canne. Dans ce scénario, nous testons l'influence du débit de données sur le réseau dans les périodes CFP et CAP. Nous utilisons deux applications qui simulent respectivement le capteur de rythme cardiaque échantillonné et un accéléromètre (tableau 3.5).

Application	Type de capteur	Inter-messages	Taille des messages	Période de transmission de trames
APP1	Rythme cardiaque	20 ms	3 Octets	CAP
APP2	Accéléromètre	100 ms	5 Octets	CFP

TABLE 3.5: Paramètres des simulations

3.3.3.1 Transmission sans BER

Les messages générés par le capteur de rythme cardiaque sont envoyés dans la CAP. Dans la CFP, les informations de l'accéléromètre sont envoyées (Figure 3.8).

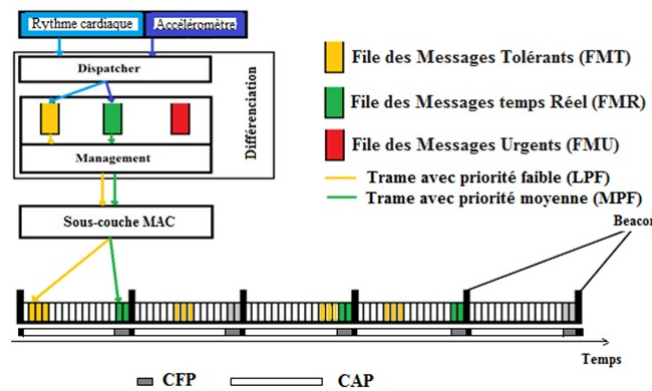


FIGURE 3.8: Exemple de transmission

Les messages qui ont une faible priorité sont empilés par la sous-couche dispatcher dans la file d'attente FMT. La sous-couche management commence à envoyer les trames LPF vers la sous-couche MAC lorsque la période CAP commence. Les messages qui ont une priorité moyenne sont empilés dans la file d'attente FMR jusqu'au commencement de la CFP, plus spécifiquement au commencement de la période réservée par le nœud. Dans la figure 3.8, on voit que le nœud contient deux applications : rythme cardiaque (rectangle bleu clair) et accéléromètre (rectangle bleu foncé), nous appellerons les deux applications APP1 et APP2 respectivement. Lorsque la sous-couche dispatcher reçoit un message de l'APP1 (ligne bleue claire) ou de l'APP2 (ligne bleue foncée), il commence par la lecture de l'entête pour connaître le profil du message. Dans le cas de l'exemple de figure 8, les

messages de l'APP1 sont envoyés vers la file **FMT** alors que ceux de l'APP2 sont dirigés vers la file d'attente **FMR**.

La sous-couche Management utilise les files d'attente **FMT** et **FMR** pour transmettre les trames dans les périodes adéquates : **CAP** ou **CFP**. Les trames de la file **FMT** sont transmises dans la période **CAP** (ligne jaune) et les trames de la file **FMR** sont servies durant la période **CFP** ; plus exactement lorsque la période réservée par le nœud commence (ligne verte).

Dans la première simulation, nous avons configuré notre simulateur (cf. tableau 3.3) pour disposer d'un environnement idéal sans erreur de transmission afin de ne mettre en évidence que les performances intrinsèques de la couche 2. La topologie utilisée est la topologie en étoile qui contient 2, 3, 6 ou 8 nœuds (incluant le coordinateur) selon les simulations. Cette configuration est utilisée également pour toutes les simulations suivantes. La taille des files d'attente (**FMT** et **FMR**) est égale à 20 trames.

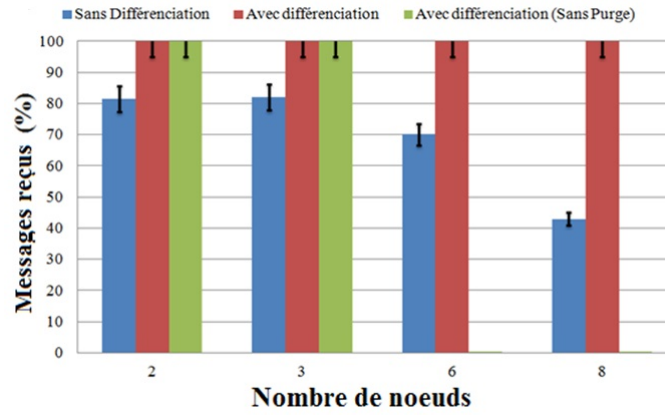


FIGURE 3.9: Taux de messages reçus dans la période GTS

La figure 3.9 montre que le taux de messages reçus pour 2 et 3 nœuds est égal à 100% pour une simulation avec la couche différenciation, ce qui dépasse le pourcentage des messages reçus dans le cas de simulations sans couche de différenciation. Mais, pour 6 et 8 nœuds, les résultats de la simulation sans différenciation deviennent meilleurs que ceux avec différenciation (sans *purge* : cf. explication ci-dessous). Ce résultat est expliqué par le fait que la couche MAC ne peut traiter qu'une seule trame à la fois. Donc, lorsqu'elle reçoit une trame pour la transmettre, elle n'accepte pas une autre trame tant que la dernière trame n'a pas été transmise ou rejetée. Ce problème est résolu par l'utilisation de la fonction *purge* que nous avons conçue et qui est appelée à la fin de chaque période **CAP** et **CFP**, ce qui permet de libérer la sous-couche MAC et rend possible le traitement d'une nouvelle trame. Cette amélioration proposée dans la couche différenciation a amélioré le pourcentage de messages reçus (passé d'une valeur proche de zéro à 100%).

La fonction *purge* donne aux couches supérieures de chaque nœud la possibilité de purger une trame de données stockée dans la sous-couche MAC avant d'être transmise. La décision de purger une trame de la file de transmission de la sous-couche MAC est prise

par la couche différenciation. De façon plus concrète, c'est la sous-couche management qui est responsable de l'instant de prise de décision de purger une trame.

La sous-couche management envoie une demande de *purge* lorsqu'elle ne reçoit pas une confirmation qui indique que la transmission est réussie ou qui indique la cause de l'échec de transmission jusqu'à la fin de la CAP. Dans ce cas, la sous-couche management considère que la sous-couche MAC traite encore la trame. Aussi, la sous-couche management envoie une demande de *purge* si elle ne reçoit pas une confirmation de la transmission de la trame dans la CFP et avant le commencement de la période CAP.

L'utilisation de la *purge* cause la perte de la trame au niveau de la couche MAC. Afin de diminuer le nombre de trames perdues lors de l'utilisation de la *purge*, notre couche de différenciation garde une copie de chaque trame transmise vers la sous-couche MAC, ce qui rend possible l'initialisation du processus de retransmission d'une trame purgée. Donc, la transmission des messages se termine obligatoirement par l'appel d'une primitive qui indique l'échec ou la réussite de l'émission.

Chaque trame est référencée par le paramètre MSDUHandle. Lorsque la couche MAC reçoit une demande de *purge* avec la référence de la trame, elle arrête le processus de transmission immédiatement si la trame est dans la file de transmission. Dans le cas de l'arrêt du processus de transmission, la couche MAC donne à la couche supérieure une réponse avec le statut SUCCESS et si la référence n'est pas valide, elle envoie INVALID_HANDLE.

Dans notre travail, la fonction *purge* est utilisée à la fin des périodes CAP et CFP afin de s'assurer que la couche MAC n'est pas occupée par le traitement d'une trame avant que la nouvelle période de transmission commence. Chaque nœud utilise la fonction *purge* à la fin de la CAP, avant le commencement de la CFP (la *purge* peut être utilisée à la fin de la CFP exactement à la fin de la période GTS réservée). La fonction *purge* est utilisée seulement en cas de besoin. Plus précisément, la *purge* est demandée si la couche différenciation a une trame qui doit être transmise dans la période CAP (ou CFP) et si elle détecte que la sous-couche MAC n'a pas transmis une trame précédente dans la période CFP (ou CAP). Dans ce cas, la couche différenciation *purge* la sous-couche MAC afin de la libérer pour traiter une nouvelle trame.

La figure 3.10 montre que le taux de messages reçus diminue avec l'augmentation du nombre de nœuds dans le réseau. Cela provient de la durée de la CAP où les nœuds tentent d'accéder au médium et de transmettre leurs informations. Cette période diminue pour chaque nœud avec l'augmentation du nombre de nœuds, puisque chaque nœud réserve des slots pour la transmission des trames MPF. Ainsi, le nombre de nœuds qui tentent d'accéder au canal dans cette même période augmente. De plus, la figure 3.10 montre que le taux de messages reçus pour la transmission avec l'utilisation de la couche différenciation avec la fonction *purge* a légèrement augmenté. Cela provient de la réinitialisation des paramètres de l'algorithme CSMA/CA due à chaque utilisation de la fonction *purge* sur les trames qui n'ont pas pu être transmises dans la période CAP. Initialement, le nombre d'essais (NB) dans l'algorithme CSMA/CA est initialisé à 0. Le

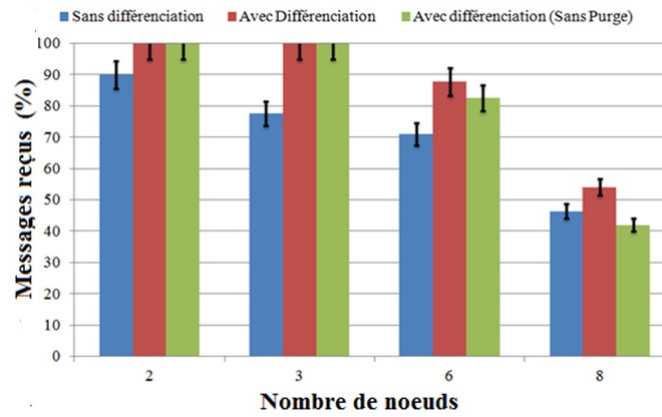


FIGURE 3.10: Nombre moyen des messages reçus dans la période CAP

nombre maximal d'essais, avant que la sous-couche MAC considère que la transmission de la trame a échoué, est égal à 3 (valeur par défaut de la norme).

Dans l'utilisation normale de la *purge*, la possibilité de garder une copie de la trame purgée n'est pas prise en considération. Donc, chaque trame purgée est considérée comme rejetée. Pour cette raison, il n'y aura pas d'influence sur le nombre de trames transmises et sur le nombre maximal d'essais de transmission puisque la trame sera rejetée définitivement. Ce n'est pas le cas dans notre solution, puisque la couche différenciation garde une copie de la trame et attend une réponse qui indique la réussite ou la cause de l'échec de transmission pour supprimer cette copie. L'utilisation de la *purge* par la couche différenciation ne mène pas au rejet de la copie de la trame, ce qui rend possible de renvoyer la trame vers la sous-couche MAC dans sa période adéquate. Cette opération de suppression et de réinitialisation de processus de transmission de la même trame donne une seconde chance pour que la trame soit transmise. Par exemple, si le nœud n'a pas pu transmettre la trame 2 fois, il ne reste donc qu'un seul essai de transmission avant que la sous-couche MAC déclare le rejet de la trame. A cet instant, on suppose que la couche différenciation demande la *purge* de cette trame afin de transmettre une autre trame. Par la suite, la couche différenciation émet une autre fois la trame purgée (puisque'elle en garde une copie). Dans ce cas, l'algorithme CSMA/CA est exécuté de nouveau et tous les paramètres seront réinitialisés : la valeur de $NB = 0$, $CW = 2$, $BE = \min(2, \minMacBE)$. Donc, cette trame a pu utiliser l'algorithme CSMA/CA deux fois avec une valeur de NB égale à 3 à chaque fois.

3.3.3.2 Transmission avec $BER = 10^{-7}$

Suite à nos simulations effectuées dans un environnement idéal, nous avons reconfiguré notre simulateur pour intégrer des erreurs de transmission afin de voir le comportement de nos propositions en environnement plus proche de la réalité. Dans la suite, nous présentons les résultats des simulations avec un $BER = 10^{-7}$ pour un nombre de nœuds égal à 2, 3, 6 et 8. Les simulations sont effectuées avec la couche différenciation sans

purge et avec la couche différenciation avec *purge*, ce qui nous permet de mettre en évidence les améliorations effectuées et leur influence sur les performances du réseau.

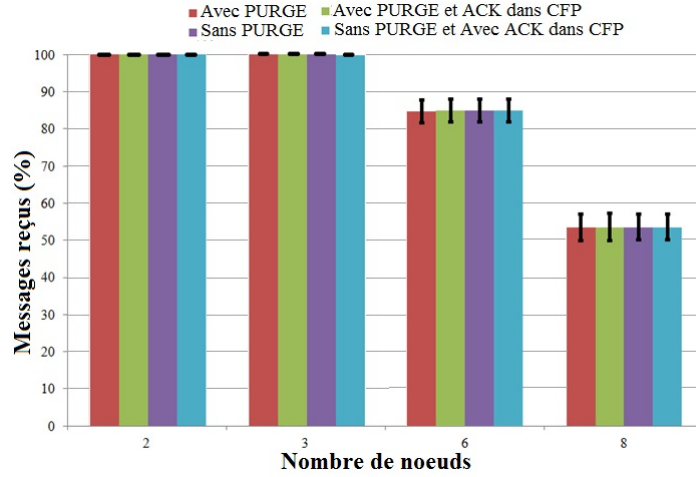


FIGURE 3.11: Taux de messages reçus dans la CAP avec $BER = 10^{-7}$

Nous pouvons identifier, dans la figure 3.11, que le taux de messages bien reçus par l'application APP1 dans les différents cas de simulations varie selon le nombre des nœuds dans le réseau. Cela provient de la durée réduite de la CAP où les nœuds tentent d'accéder et transmettre leurs informations. Seul le délai de bout en bout est légèrement amélioré (cf. figure 3.12) pour 2 et 3 nœuds lorsqu'on utilise la fonction *purge*. Cela est dû à l'initialisation du NB, BE et CW à chaque fois que le nœud émetteur utilise la *purge* pour libérer la couche MAC afin de transmettre les paquets de l'APP2. Par la suite, le nœud renvoie le paquet une fois de plus avec les paramètres initiaux de l'algorithme CSMA/CA (NB, CW, BE). Ainsi, le nœud peut avoir plus de chance de trouver le canal libre puisqu'il existe des nœuds où la couche différenciation n'a pas purgé la trame. Dans ce cas là, les nœuds vont garder la même valeur de BE (à chaque fois lorsqu'ils trouvent le canal occupé, la valeur de $BE = \min(BE+1, \text{macMaxBE})$, ce qui donne plus de chance aux nœuds qui ont effectué une *purge* d'accéder au canal puisque la valeur de BE est réinitialisée ($BE = \min(2, \text{macMinBE})$). Les nœuds qui vont réinitialiser leurs paramètres de l'algorithme CSMA/CA ont une durée d'attente plus petite, donc, plus de chance de transmission réussie. Ceci diminue le nombre de trames rejetées et le nombre d'échecs de transmission.

Le cas de l'utilisation de la *purge* est composé de trois sous-cas :

- 1^{er} sous-cas : un seul nœud a utilisé la *purge* dans le réseau, M nœuds n'ont pas utilisé la fonction *purge* et L nœuds effectuent leur premier essai de transmission : le nœud qui a utilisé la *purge* entre en concurrence avec les nœuds qui effectuent leur première transmission de trames. Donc, seul le nœud qui a purgé une trame et les nœuds qui effectuent leurs premières transmissions utilisent un $BE = \min(2, \text{macMinBE})$ alors que les autres utilisent un $BE = \min(BE+1, \text{macMaxBE})$. Dans ce cas, le nœud qui a utilisé la *purge* est le plus prioritaire, ainsi que les nœuds

qui vont transmettre pour la première fois puisqu'ils ont tous une grande chance d'avoir la plus petite valeur de backoff.

- 2^{ème} sous-cas : **N** nœuds ont utilisé la *purge*, **M** nœuds n'ont pas utilisé la *purge* et **L** nœuds effectuent leur premier essai de transmission : **N** nœuds vont initialiser les paramètres de l'algorithme CSMA/CA. Dans ce sous-cas, **N + L** nœuds vont utiliser un **BE** = min (2, macMinBE) alors que les autres vont utiliser un **BE** = min(**BE**+1, macMaxBE). Donc, **N + L** nœuds ont plus de chance d'accéder au médium que les **M** nœuds.
- 3^{ème} sous-cas : tous les nœuds utilisent la fonction *purge* : dans ce sous-cas, tous les nœuds dans le réseau ont effectué une initialisation de l'algorithme CSMA/CA. Ceci signifie que tous les nœuds vont avoir une petite valeur de **BE**. Cette étape représente une initialisation de transmission dans tout le réseau, ce qui génère plusieurs risques de collision. Ce cas ne devrait pas se produire très souvent.

Remarque : $N + L + M \leq 7 \text{ nœuds}$

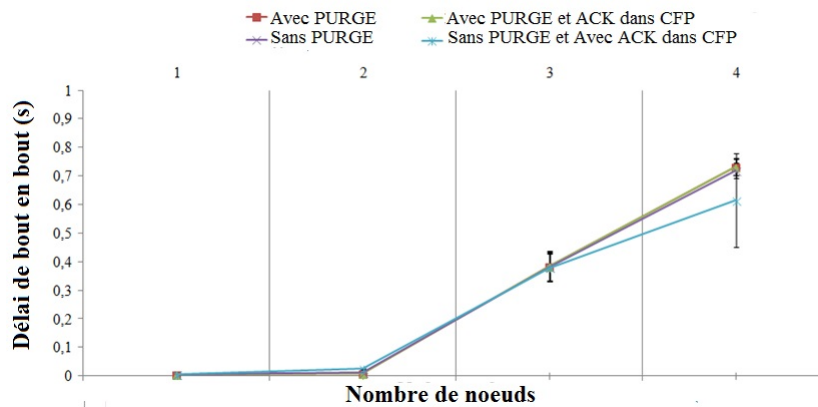
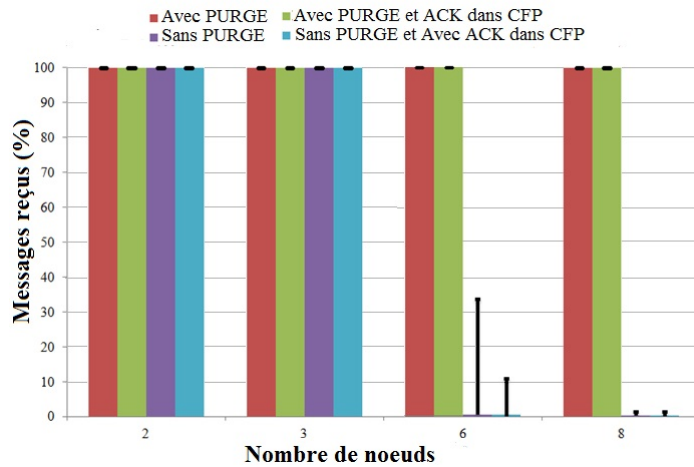


FIGURE 3.12: Délai moyen de bout en bout dans la CAP avec $BER = 10^{-7}$

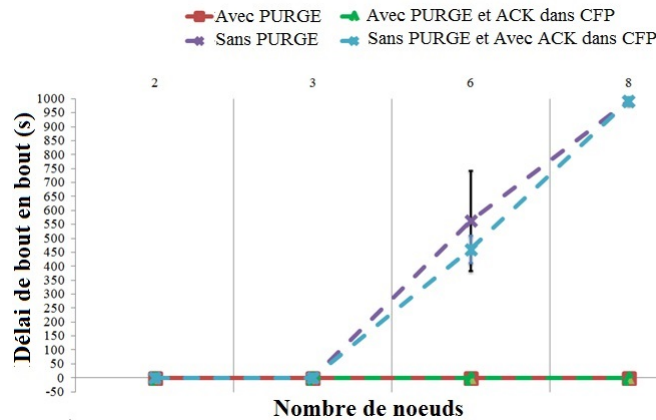
A partir des deux courbes (figure 3.11 et figure 3.12), nous pouvons conclure que dans la CAP, il n'y a pas une amélioration significative avec l'utilisation de la *purge* au niveau du nombre de messages reçus par l'application APP1 du coordinateur. Par contre, il faut signaler que le délai de bout en bout pour 2 et 3 nœuds est légèrement amélioré. Pour 6 et 8 nœuds, le délai moyen de bout en bout avec l'utilisation de la couche de différenciation sans *purge* reste légèrement meilleur, mais en contre partie, nous avons une perte de performance dans la CFP puisque le nombre de trames transmises est proche de zéro (voir Figure 3.9).

Après l'étude que nous avons effectuée sur la transmission dans la CAP, nous allons nous intéresser maintenant à la période CFP qui est généralement réservée pour la transmission des messages qui demandent un plus fort niveau de QoS.

La figure 3.13 montre que l'utilisation de la *purge* permet la réussite de transmission pour tous les messages dans le cas où l'application APP2 demande un acquittement à chaque

FIGURE 3.13: Taux de messages reçus dans la CFP avec $BER = 10^{-7}$

trame émise et bien reçue. Même sans la gestion de l’acquittement (et retransmission de la trame de données si échec), le pourcentage de réussite (donc dès la première émission) est très proche de 100% dans tous les cas. Par contre, dans le cas où le nœud n’utilise pas la *purge*, le pourcentage est à 100% seulement pour 2 et 3 nœuds (cf. tableau 3.13). Pour 6 et 8 nœuds, le pourcentage de paquets reçus est presque nul, ce qui montre bien l’utilité de l’utilisation de la fonction *purge* par la couche différenciation. De plus, le délai moyen de bout en bout est réduit d’une manière très significative : il est passé de 475 ms à 50 ms pour 6 nœuds (cf. figure 3.14).

FIGURE 3.14: Délai moyen de bout en bout des messages reçus dans la CFP avec $BER = 10^{-7}$

3.3.3.3 Explication du fonctionnement de la purge

La figure 3.15 illustre un exemple pour clarifier la problématique des transmissions dans des périodes différentes à travers la même couche MAC. Dans la figure 3.15 les périodes de disponibilité de la sous-couche MAC sont colorées en blanc, alors que la couleur orange est dédiée aux périodes d’indisponibilité. Dans le cas de l’utilisation de la couche de différenciation, la sous-couche management n’envoie une trame à la sous-couche MAC

que lorsqu'elle est disponible. Dans une situation parfaite, la sous-couche MAC transmet une trame dans la période **CAP** et une autre dans la période **CFP** (cf. figure 3.15, la période de transmission d'une trame LPF dans la **CAP** est colorée en violet, alors que celle de MPF est colorée en orange). Lorsqu'il existe une grande charge dans le réseau, la sous-couche MAC tente de transmettre le paquet NB fois (le nombre d'essais ne dépasse pas 3), pour cette raison elle garde la trame pendant toute la période d'essai. La figure 3.15 montre bien que pendant les supertrames 2 et 3, la sous-couche MAC est occupée par la transmission d'une trame LPF, donc, elle ne demande pas une trame à la sous-couche management. La sous-couche MAC garde la trame pendant toute la période **CFP**, ce qui bloque les autres trames de la file MPF au niveau de la couche différenciation. Elles ne seront transmises que lorsque la sous-couche MAC se libère. Cette problématique a été résolue par l'utilisation de la fonction *purge* puisque cette fonction permet la libération de la sous-couche MAC, et donc la possibilité de transmettre les trames dans les périodes adéquates sans être bloquées par des autres transmissions.

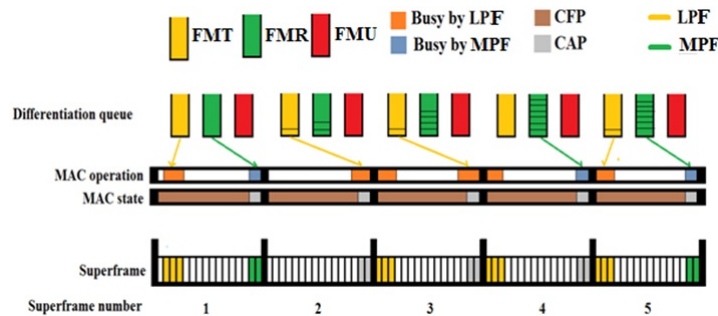


FIGURE 3.15: Exemple de transmission sans l'utilisation de la purge

Cette nouvelle fonction est ajoutée à l'ensemble des fonctionnalités fournies par la couche management. La figure 3.16 présente un cas simple de l'utilisation de la couche différenciation. Le premier schéma (figure 3.16 (a)) présente les différents éléments que nous utilisons dans la présentation de l'exemple. Le nœud est composé de quatre couches. La couche application contient deux applications : APP1 qui génère des messages à faible priorité, et APP2 qui génère des messages qui ont une priorité moyenne. La couche différenciation contient deux sous-couches (dispatcher et management) et trois mémoires ou buffers pour sauvegarder les copies des trames transmises vers la sous-couche MAC.

La figure 3.16 (b) présente les étapes de transmission d'un message. En premiers lieu, APP1 envoie un message (étape 1) vers la couche différenciation. Dès la réception des messages, la sous-couche dispatcher prend en charge la vérification et la classification des messages (étape 2). Après cette étape de vérification, le message sera empilé dans la file d'attente adéquate (étape 3). Lorsque la période temporelle de transmission associée au bon type de file d'attente commence, la sous-couche management envoie une trame de la file vers la sous-couche MAC (étape 4) en gardant une copie dans la mémoire associée à la file d'attente. Lorsque le message est bien transmis (étape 5), la sous-couche MAC

envoie une indication à la sous-couche management pour l'informer. Alors, la sous-couche management supprime la copie et transmet une autre trame vers la sous-couche MAC.

Remarque : Les trames LPF seront transmises dans la CAP. Au début de cet exemple, toutes les files d'attente sont vides et la couche MAC ne traite aucune trame.

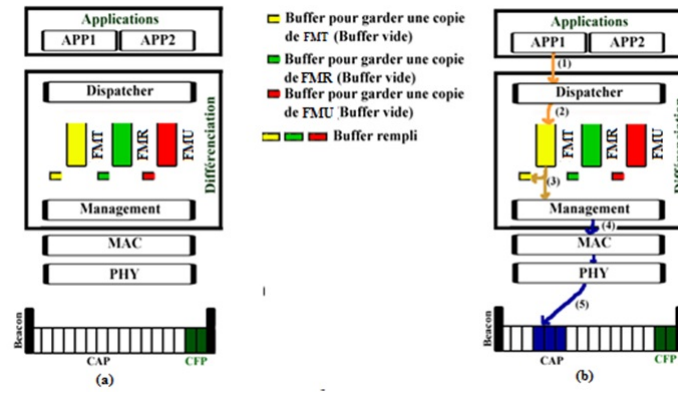


FIGURE 3.16: Exemple de transmission avec l'utilisation de la couche différenciation

Après l'explication de l'exemple présenté dans la figure 3.15, nous expliquons un autre exemple qui représente un cas de l'utilisation de la *purge*. La figure 3.17(a) reprend exactement les mêmes étapes de la figure 3.16(b) sauf pour l'étape 5 qui a été supprimée puisqu'il existe plusieurs nœuds dans le réseau (il existe deux autres nœuds qui tentent de transmettre leurs données). Pour cette raison, le nœud présenté dans la figure 3.17(a) garde la trame au niveau de la sous-couche MAC afin de réussir la transmission.

Dans la figure 3.17(b), APP2 envoie un message vers la couche différenciation. Dès la réception, la sous-couche dispatcher envoie le message vers la file FMR. À la fin de la période CAP, la sous-couche management a remarqué qu'elle n'a pas reçu une réponse qui concerne la transmission de la trame dans la période CAP. Donc, la sous-couche management considère que la sous-couche MAC n'a pas pu transmettre la trame et elle envoie une demande de *purge* (étape 8). Lorsque la sous-couche MAC reçoit la demande, elle supprime la trame de la file de transmission, change son état d'occupé à libre et envoie une réponse vers la sous-couche différenciation (étape 9). Dès que la sous-couche management reçoit la réponse qui confirme l'exécution de la *purge*, elle commence la préparation pour l'envoi d'une trame de la file FMR dans la CFP (figure 3.17(d), étape 10). Lorsque la sous-couche MAC reçoit la trame, elle la transmet dans la période réservée par le nœud et elle envoie une réponse pour informer la sous-couche management que la transmission est terminée avec succès. La sous-couche management supprime la copie de la mémoire et prépare une autre trame si la durée de la CFP n'est pas terminée.

Après la réception d'un beacon, la sous-couche management recopie la trame de la mémoire associée à la file FMT et l'envoie vers la sous-couche MAC (figure 3.18, étapes 1 et 2).

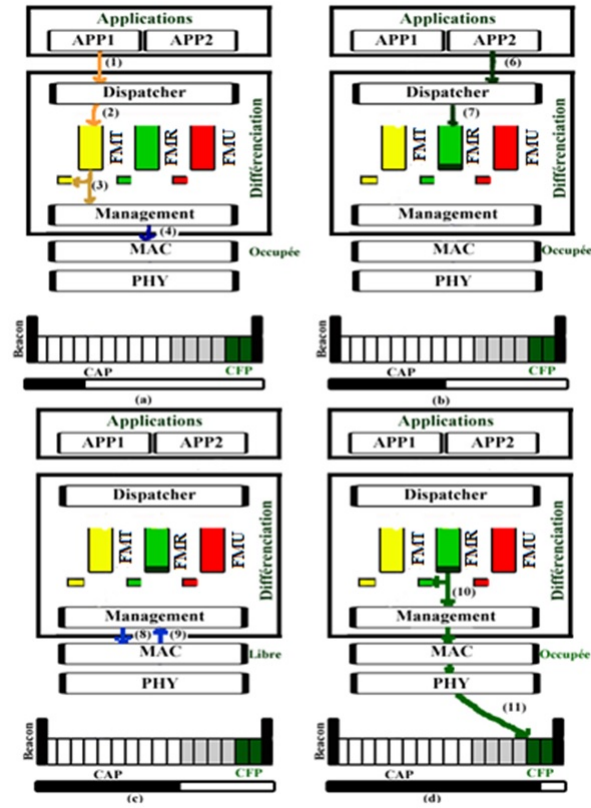


FIGURE 3.17: Exemple de transmission avec l'utilisation de la purge

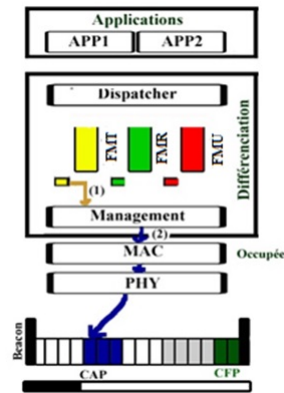


FIGURE 3.18: Suite de l'exemple présenté dans la figure 3.17

L'influence de l'utilisation de la fonction *purge* réduit le pourcentage de trames en échec, qui passe d'une valeur supérieure à 1% à une valeur de l'ordre de 0.8%. Cela est dû à la réinitialisation des paramètres de la transmission (NB, CW et BE) et à la bonne gestion des périodes de transmission par l'utilisation de la couche différenciation qui arbitre le passage des trames vers la sous-couche MAC selon les périodes de transmission et le type de la trame. Le pourcentage de trames en échec (voir figure 3.19) est très faible (de l'ordre de 1,6%, ce qui représente 5600 paquets sur les 350000 paquets transmis pendant 1000 secondes, et pour les 8 nœuds) et l'augmentation légère du nombre de messages qui ne sont pas rentrés dans la file d'attente FMT (augmentation d'une valeur supérieure ou égale à 0,7%) (voir figure 3.20). Pour ces raisons, il n'y a pas une augmentation du taux

des messages bien transmis dans la période CFP. Mais cette amélioration est significative au niveau du délai moyen de bout en bout puisque le nombre de retransmissions des trames a diminué (le nombre d'essais de transmissions effectué par le nœud a diminué). Donc, le temps d'attente au niveau de la file diminue d'une manière très significative.

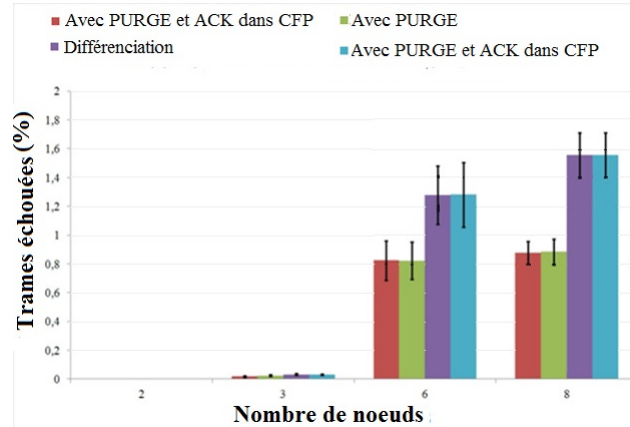


FIGURE 3.19: Pourcentage des trames en échec

Le taux de messages qui n'entrent pas dans la file d'attente (figure 3.20 pour la file FMT) a légèrement augmenté, ce qui réduit les chances d'accroître le nombre de messages bien reçus et ce qui permet de garder les mêmes taux de messages bien reçus par le coordinateur, en plus de toutes les améliorations effectuées au niveau du délai moyen de bout en bout et du nombre de trames échouées.

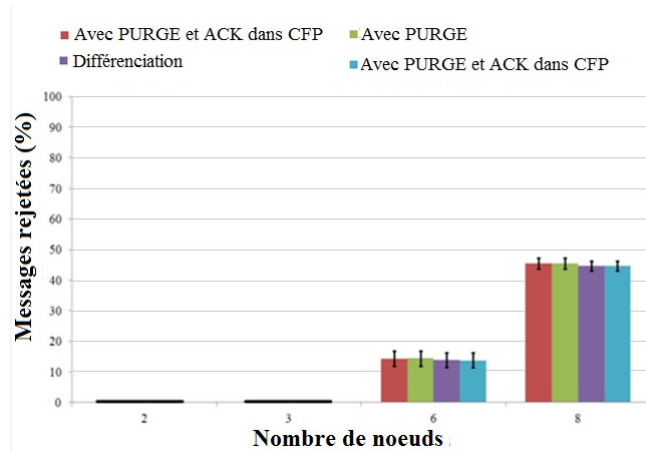


FIGURE 3.20: Nombre moyen de trames rejetées par la file FMT avec $BER = 10^{-7}$

3.3.3.4 Impact du BER

Après cette étude comparative entre l'utilisation de la couche différenciation avec la *purge* et sans la *purge*, nous avons remarqué que l'utilisation de la couche différenciation avec la *purge* permet d'atteindre des résultats intéressants, essentiellement pour la période CFP. La gestion des acquittements dans la période CFP n'a pas de grande influence sur les performances de réseau. Finalement, l'utilisation d'un environnement très optimiste

dans un environnement sans fil avec un BER égal à 10^{-7} n'a pas une grande influence sur les performances offertes par la couche différenciation avec *purge* (en comparaison avec un médium parfait). Pour cette raison, nous allons effectuer des simulations pour des BER plus réalistes, en prenant des valeurs de 10^{-5} et 10^{-3} .

Les simulations suivantes sont effectuées uniquement avec la couche différenciation avec *purge* puisqu'elle offre des résultats meilleurs que ceux des autres propositions (sans différenciation et avec différenciation sans *purge*).

Dans cette partie, nous utilisons la même configuration réseau, avec juste la valeur de BER modifiée. Notre objectif est de voir l'influence des erreurs au niveau de la transmission sur notre couche de différenciation.

La figure 3.21 montre que notre couche de différenciation pour une valeur de BER égale à 10^{-5} offre un nombre moyen de messages reçus très proche de ceux présentés dans les figure 3.2 et 3.6 (avec un médium parfait), nous pouvons donc déduire que les BER égaux à 10^{-7} et 10^{-5} n'avaient pas un grand impact sur les performances du réseau. Pour un BER égal à 10^{-3} , les performances du réseau ont diminué et le pourcentage moyen de messages reçus est passé d'une valeur supérieure à 80% pour un BER égal à 10^{-7} et 10^{-5} , à une valeur inférieure à 80% pour 6 nœuds, ce qui est tout à fait normal, mais reste encore acceptable.

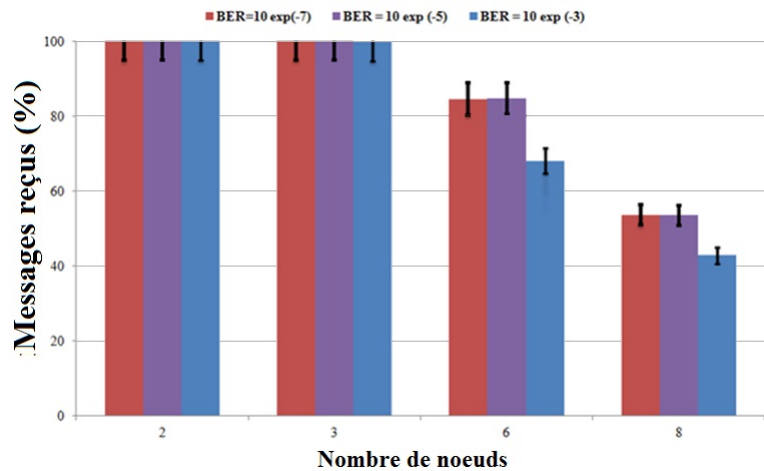


FIGURE 3.21: Nombre moyen de messages reçus dans la CAP

La figure 3.22 montre que le blocage des trames dû aux problèmes de retransmission ou de canal occupé, est la cause du débordement des files d'attente. La figure 3.23 montre les quatre cas de base qui causent la retransmission de la trame, ayant comme conséquence l'augmentation du temps d'attente dans la file d'attente et l'augmentation du risque de débordement de la file d'attente. La figure 3.23 (a) et (b) présente les deux premiers cas de retransmission pouvant avoir lieu dans le réseau. Dans ces deux cas, la retransmission de la trame est effectuée parce que l'émetteur n'a pas reçu un ACK valide à cause d'un problème de transmission de la trame ou de l'ACK. La figure 3.23 (c) et (d) présente les cas de retransmission dues aux collisions qui peuvent avoir lieu pour une transmission lors de l'émission d'une trame ou d'un ACK.

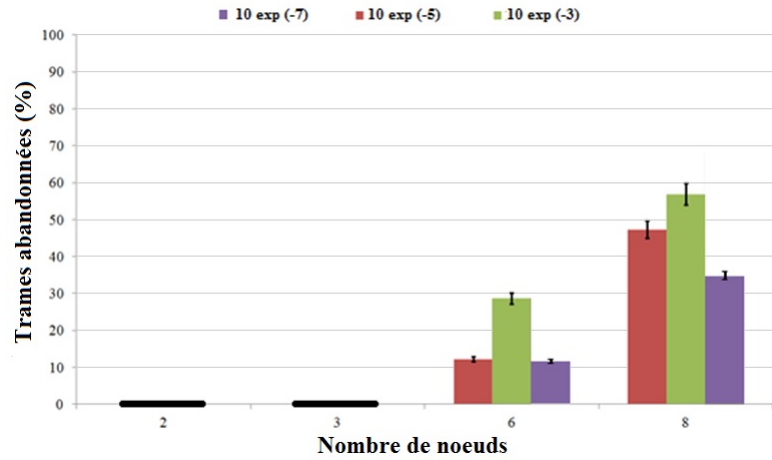


FIGURE 3.22: Nombre moyen de messages qui ne sont pas rentrés dans la file FMT

L'augmentation de la valeur du BER est accompagnée par une augmentation du nombre de messages qui n'entrent pas dans la file **FMT**.

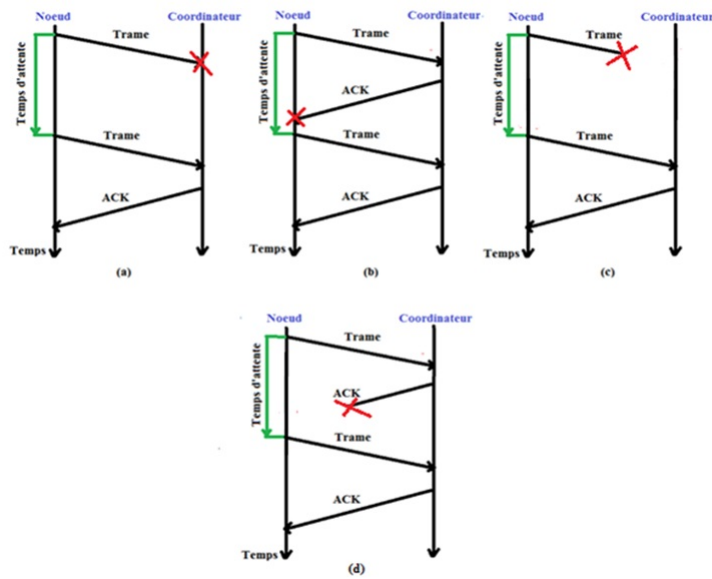


FIGURE 3.23: Différents cas de retransmission

La figure 3.24 montre que la valeur de BER n'a pas d'influence majeure sur notre couche de différenciation.

Le pourcentage des messages reçus (cf. figure 3.25) dans la période **CFP** a diminué pour une valeur de $BER = 10^{-3}$. Le coordinateur a reçu au moins 80% des paquets émis, ce qui nous permet de conclure que notre couche de différenciation résiste bien à de très mauvaises valeurs de BER. Dans la figure 3.26, on remarque que le nombre de paquets rejetés est égal à zéro, ce qui montre bien que la diminution du pourcentage de paquets reçus dans la période **CFP** est due aux seules erreurs de transmission.

Suite aux simulations effectuées, nous avons noté que notre couche de différenciation permet d'avoir une bonne gestion de la transmission en accordant à chaque type de

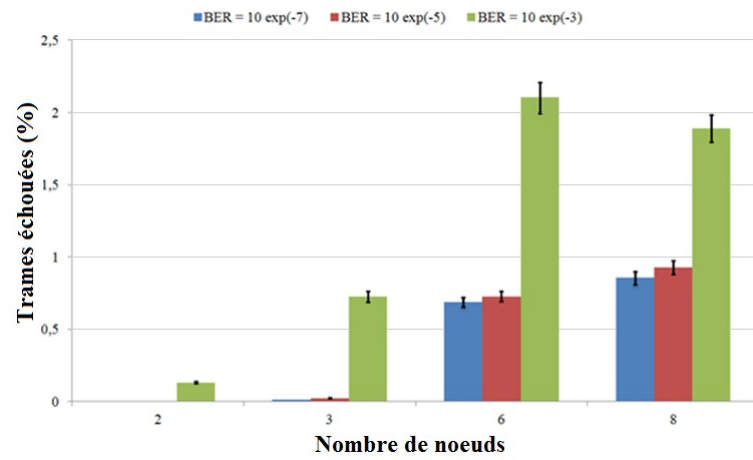


FIGURE 3.24: Nombre moyen de trames rejetées par la sous-couche MAC à cause d'échecs de transmission

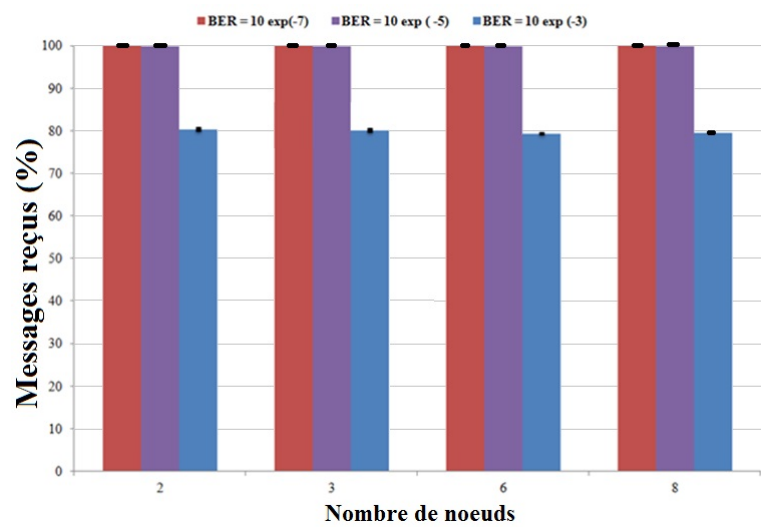


FIGURE 3.25: Nombre moyen de trames reçues dans la période CFP sans ACK

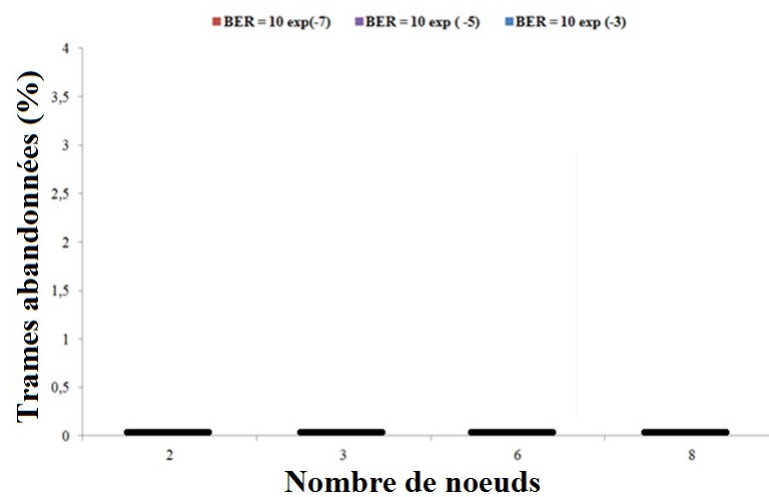


FIGURE 3.26: Nombre moyen de trames rejetées par la file FMT

trame l'accès à la période adéquate sans être influencé par d'autres trames. Ceci n'est pas le cas pour les simulations sans la couche différenciation où la sous-couche MAC traite toutes les trames de la même façon sans considérer l'importance des périodes CAP et CFP.

L'ajout de l'utilisation de la fonction *purge* par la couche différenciation a amélioré d'une manière très significative le pourcentage des messages reçus dans la CFP qui atteint 100%, ce qui montre la bonne gestion des périodes CAP et CFP.

Nous avons effectué des tests avec des valeurs de BER égales à 10^{-7} , 10^{-5} et 10^{-3} . Ces tests ont bien montré que pour un BER égal à 10^{-7} ou 10^{-5} , notre couche de différenciation résiste très bien et offre de bons résultats pour les périodes CAP et CFP. Par contre, pour un très mauvais BER égal à 10^{-3} , nous avons noté une diminution des performances avec une augmentation du nombre de messages qui ne peuvent pas entrer dans la file FMT à cause du débordement de cette dernière, et des files qui débordent à cause de l'augmentation du nombre d'échecs de transmission (car 3 tentatives atteintes), pour les transmissions dans la CAP. La diminution du nombre de paquets reçus dans la période CAP est due alors à l'augmentation des erreurs de transmission. Nous sommes à la limite de l'efficacité de l'empilement protocolaire.

3.3.4 Présence d'une alerte dans le réseau

Dans cette partie, nous simulons l'apparition d'une alerte dans une canne du réseau. Les paramètres de la simulation, ainsi qu'un rappel sur les caractéristiques des capteurs utilisés sont présentés dans le tableau 3.6.

Paramètres		Valeurs
Durée de la simulation		5 heures
Nombre de répétitions		4
Taille de File d'attente	FMR	10
	FMT	
	FMU	
Application 1	Taille du message	4 octets
	Durée d'inter-arrivée des messages	4 min
	Profil	2
	Capteur	capteur de température de la main
	Mode de transmission	CAP
Application 2	Taille du message	5 octets
	Durée d'inter-arrivée des messages	2 s
	Profil	6
	Capteur	accéléromètre
	Mode de transmission	CFP
Application 3	Taille du message	3 octets
	Durée d'inter-arrivée des messages	100 s
	Profil	9
	Capteur	capteur de température de la main
	Mode de transmission	CFP et CAP

TABLE 3.6: Paramètres du réseau pour une simulation d'alerte

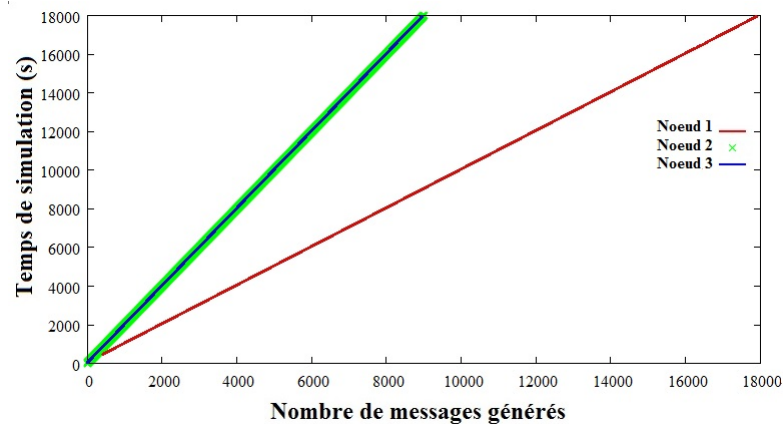


FIGURE 3.27: Nombre de messages générés par l'application 1

Les figures 3.27 et 3.28 présentent le nombre de messages générés par l'application 1 et 2 pendant la simulation. On identifie que le nombre de messages générés par le nœud 1 (qui représente la canne 1) est deux fois supérieur au nombre de message générés par les nœuds numéros 2 et 3. Cette différence s'explique par la présence d'un état critique dans le nœud 1, donc le nombre de messages générés sera deux fois plus grand que celui des nœuds dans un état ordinaire.

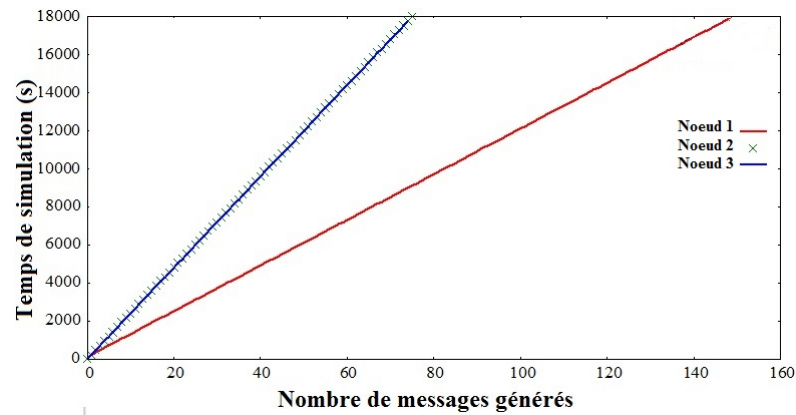


FIGURE 3.28: Nombre de messages générés par l'application 2

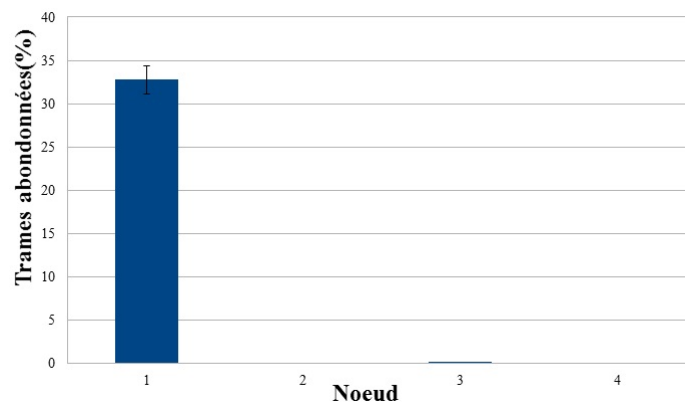


FIGURE 3.29: Pourcentage des trames non acceptées par la file FMR

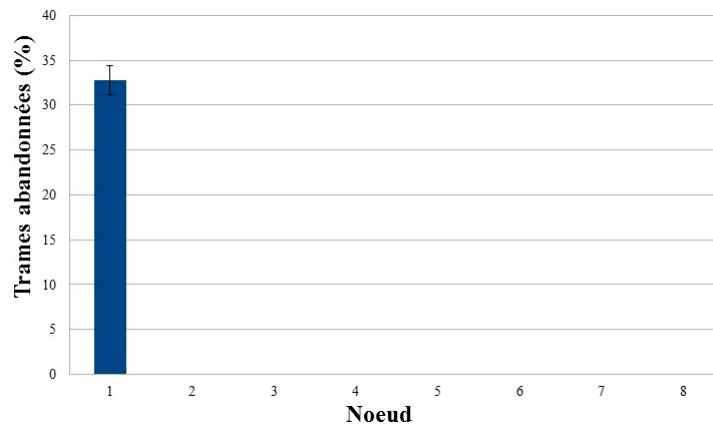


FIGURE 3.30: Pourcentage des messages non acceptés par la file FMR

Lorsque l'état critique se déclenche dans une canne, le nombre de messages générés par cette dernière est multiplié par 2. Cette augmentation génère une modification au niveau des paramètres initiaux utilisés pour calculer les valeurs de [BO](#) et [SO](#). Donc, la probabilité que les messages ne soient pas capables d'entrer dans la file d'attente augmente pour la canne qui contient l'état critique. Les figures [3.29](#) et [3.30](#) présentent le nombre des messages qui n'ont pas pu entrer dans la file d'attente [FMR](#). À partir des

figures, nous identifions bien que la canne n° 1 est dans l'état critique, ce qui a causé l'augmentation de la fréquence de génération des messages (dont la période est passée de 2s à 1s). Cette augmentation est la cause de la perte de plus de 30% des trames, contrairement aux autres nœuds dans le réseau où le pourcentage de pertes est égal à 0% (voir figure 3.29 et 3.30).

Afin de surmonter cette problématique, la couche différenciation recalcule les valeurs de **BO** et **SO** lors de la réception de l'alerte. Ensuite, elle envoie ces valeurs à la couche MAC pour les retransmettre aux différentes cannes de réseau dans le beacon. Dans notre cas, les nouvelles valeurs de **BO** et **SO** seront 10 et 6 respectivement. Ce changement de configuration implique un changement au niveau de la réservation des slots **GTS**. Toutes les informations nécessaires, comme les nouvelles valeurs de **BO** et **SO** et les nouvelles périodes de réservation, pour maintenir la stabilité et le fonctionnement de réseau et éviter tous types de perturbation seront envoyées dans le beacon avec une indication pour que les nœuds les prennent en considération dès la réception.

Les figures 3.31, 3.32, 3.33 et 3.34 montrent que le passage à l'état critique influence énormément le nœud qui l'engendre. Les deux figures montrent que le changement des valeurs de **BO** et **SO** a une influence positive au niveau des performances du réseau, puisque, avec les nouveaux paramètres, le nœud 1 (qui est dans l'état critique) a pu transmettre tous les messages dans la période **CFP** sans avoir le moindre problème.

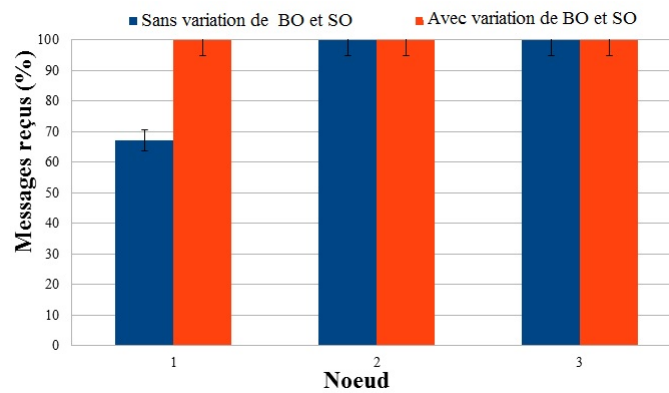


FIGURE 3.31: Pourcentage de nombre moyen des messages reçus dans la CFP

Le nombre maximal de messages reçus a diminué de 50% lors du changement de **BO** et **SO**. Cela correspond à la diminution de la période entre 2 **GTS** successifs pour chaque nœud.

Pour les messages transmis dans la période **CAP**, il n'existe pas de problème de rejet des messages, puisque la périodicité de génération est très lente (240 s). Même si le nœud demande une accélération des transmissions des trames, la période de génération reste faible (120 s), le nœud peut donc toujours avoir le temps nécessaire pour transmettre les trames de la file d'attente **FMT**.

Le temps d'accès au medium nécessaire reste aléatoire. Avec la solution proposée pour augmenter la priorité de la canne en état critique, le nombre d'essais pour gagner l'accès

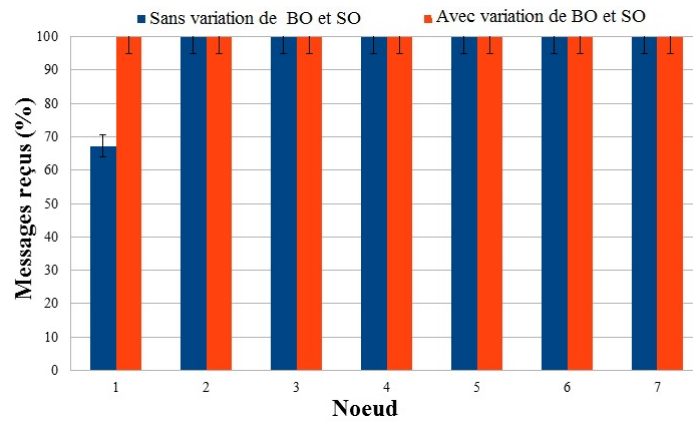


FIGURE 3.32: Pourcentage de nombre moyen des messages reçus dans la CFP pour 7 noeuds

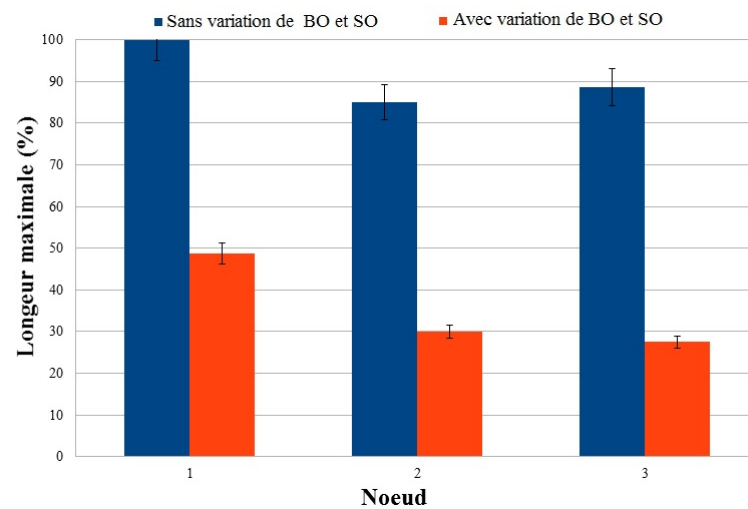


FIGURE 3.33: Longueur moyenne maximale de la file FMR pour 3 noeuds

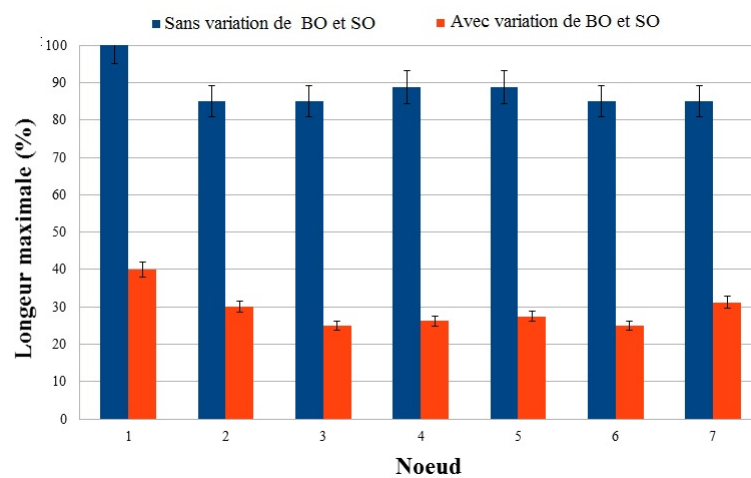


FIGURE 3.34: Longueur moyenne maximale de la file FMR pour 7 noeuds

au médium diminue, ce qui signifie que la canne gagnera dans la plupart des cas l'accès au médium (voir figure 3.35 et 3.36).

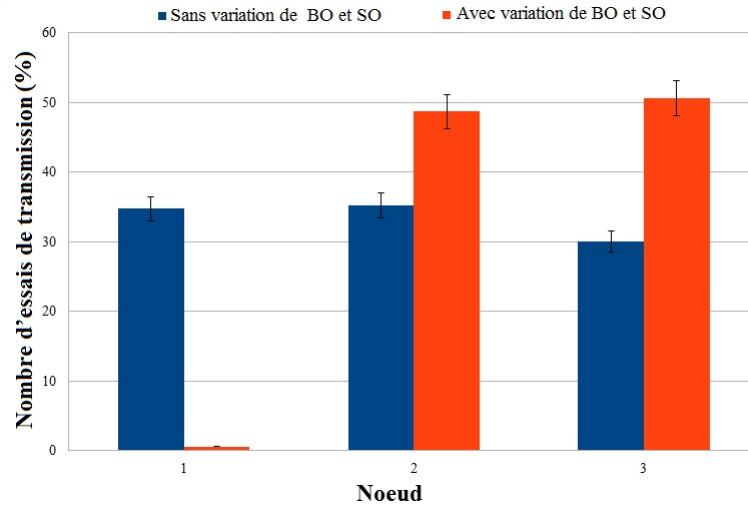


FIGURE 3.35: Nombre moyen d'essais de transmission pour 3 noeuds

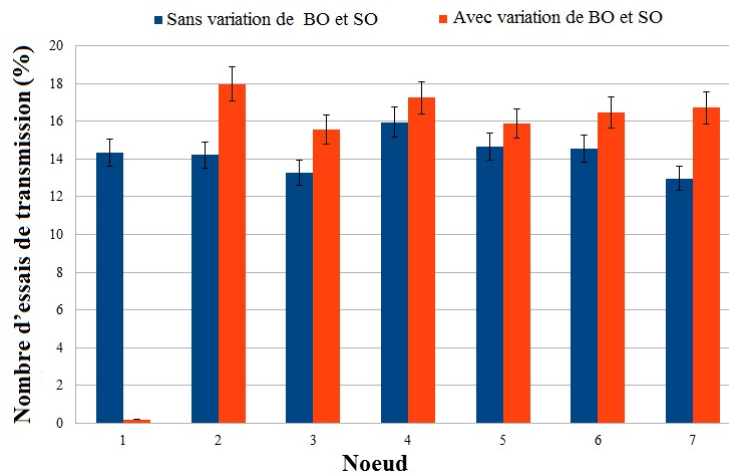


FIGURE 3.36: Nombre moyen d'essais de transmission pour 7 noeuds

3.4 Bilan

Les résultats des simulations présentées dans ce dernier chapitre ont montré que nos solutions améliorent fortement les performances du réseau et satisfont les exigences des différents capteurs de cannes dans le réseau.

La couche différenciation joue un rôle important dans la gestion et la synchronisation des transmissions des trames selon leurs profils. De plus, elle permet la bonne transmission des trames dans les périodes CAP et CFP, ce qui permet une utilisation efficace de la bande passante et permet de profiter pleinement de la composition de la supertrame dans la norme IEEE 802.15.4 native, sans modification majeure de cette dernière.

Suite aux simulations effectuées, nous avons noté que notre couche de différenciation permet d'avoir une bonne gestion de la transmission en accordant à chaque type de paquet l'accès à la période adéquate sans être influencé par d'autres paquets. Ceci n'est pas le cas pour les simulations sans la couche différenciation où la sous-couche MAC

traite toutes les trames de la même façon sans considérer l'importance des périodes CAP et CFP.

L'utilisation de la fonction *purge* par la couche de différenciation a amélioré, d'une manière très significative, le pourcentage des paquets reçus dans la CFP qui atteint 100% avec l'utilisation des fonctions pour conserver une copie de la trame transmise vers la couche MAC au niveau de la couche différenciation.

Nous avons, aussi, effectué des tests avec des valeurs de BER égales à 10^{-7} , 10^{-5} et 10^{-3} . Ces tests ont montré que pour un BER égal 10^{-7} ou 10^{-5} , notre couche de différenciation offre de bons résultats. Par contre pour un BER égal à 10^{-3} , nous avons noté une diminution des performances avec une augmentation du nombre de messages qui ne peuvent pas entrer dans la file FMT à cause du débordement de cette dernière. Ce débordement des files est le résultat de l'augmentation du nombre d'échecs de transmission la CAP. La diminution du nombre de paquets reçus dans la période CFP est due alors à l'augmentation des erreurs de transmission. Un BER de 10^{-3} reste un cas extrême, peu réaliste.

L'état critique est caractérisé par une augmentation du nombre de messages générés par les applications de la canne. Cette augmentation demande un traitement et des paramètres spéciaux qui seront accordés par le coordinateur. Dans les simulations effectuées, le nombre de trames qui n'ont pas pu entrer dans la file d'attente FMR est très important dans la canne qui a généré l'alerte. Une variation des valeurs de BO et SO a permis de regagner les performances initiales du réseau. Aussi, l'utilisation des nouvelles valeurs de BO et SO adaptées à la situation de l'état critique, et le nombre de trames dans la file FMR qui attendent d'être servies, a diminué.

Afin de donner une priorité aux nœuds qui sont en état critique, la couche différenciation offre la possibilité de privilégier ces nœuds dans la période CAP. Ce privilège consiste à interdire les nœuds qui ne sont pas en alerte d'avoir une valeur de *Backoff* plus petite que celle des nœuds qui ont un état critique. Les simulations ont montré que la canne qui a annoncé l'état d'alerte accède rapidement au réseau par rapport aux autres nœuds et à l'utilisation de la couche MAC 802.15.4 sans la couche différenciation.

3.5 Conclusion

Dans ce dernier chapitre, nous avons présenté les simulations effectuées avec et sans la couche différenciation. Nos simulations ont montré l'efficacité de l'utilisation de la couche de différenciation, ainsi que l'importance de cette couche pour différencier et améliorer les performances d'un réseau qui contient une multitude de capteurs biométriques. La couche différenciation a rendu la couche MAC de 802.15.4 capable de s'adapter aux besoins des applications d'une manière dynamique.

Conclusion générale et perspectives

Conclusion générale

Les changements d'habitude des personnes, lorsqu'elles atteignent le troisième âge, jouent un rôle important dans la dégradation de leur état de santé. Les nouvelles technologies ont permis de proposer des solutions qui offrent la possibilité de surveiller et d'effectuer le contrôle d'une manière non intrusive. Dans notre thèse, nous avons travaillé sur une idée évolutive qui propose l'utilisation de la canne comme un élément de suivi et de contrôle des personnes âgées. Afin de réaliser les objectifs proposés, la canne doit être équipée par une multitude de capteurs biométriques.

Après une étude détaillée des technologies et des architectures qui peuvent être utilisées avec les projets *e-santé*, nous avons proposé une topologie multi-niveaux. Nous avons utilisé plusieurs technologies de communication afin d'établir un lien permanent entre ces niveaux. Notre architecture est donc en même temps multi-niveaux et multi-interfaces. Suite à cette proposition, nous avons identifié l'importance de la liaison entre les cannes et le [CMAP](#). Pour cette raison, nous avons concentré la suite de nos travaux sur la communication entre les cannes et le [CMAP](#).

Dans ce niveau, une multitude d'informations générées par des capteurs ont des caractéristiques différentes. Cette diversité complique le traitement effectué pour satisfaire les contraintes de transmissions exigées. Notre étude sur les caractéristiques des capteurs a révélé l'existence des traits communs, qui nous ont permis de classer les capteurs en dix profils. Cette classification donne une vue globale sur les besoins de chaque catégorie de capteurs. Nous avons alors pu associer à chaque profil la période de transmission adéquate : [CAP](#), [CFP](#) ou [CAP/CFP](#).

À partir de cette classification, nous avons fait germer l'idée d'ajouter une couche de différenciation qui implémente l'étape de classification pour la couche MAC. La couche de différenciation est la seule couche capable de différencier les trames et de les synchroniser avec leurs périodes de transmission adéquates.

Le choix des périodes de transmission ne garantit pas la satisfaction des applications puisque la durée et le temps qui séparent deux périodes de transmission dépendent des

valeurs de **BO** et **SO**. Nous avons alors étudié l'influence de la variation de **BO** et **SO** sur les performances du réseau, en particulier le débit de transmission et la durée de la période d'inactivité. Les analyses que nous avons effectuées ont permis de connaître les intervalles des valeurs ou les valeurs exactes de **BO** et **SO** qui doivent être associées à chaque profil selon les critères de débit et de périodicité de génération des messages.

Dans la norme 802.15.4, les valeurs de **BO** et **SO** sont choisies par les couches supérieures au début de l'application de transmission. Dans notre solution, les valeurs de **BO** et **SO** sont calculées par la sous-couche management. Cette solution dépend essentiellement des caractéristiques de l'application qui sera utilisée, et qui sert de base pour calculer des valeurs optimales de **BO** et **SO**. Dans notre cas, nous utilisons les périodes **CAP** et **CFP** qui sont associées respectivement aux techniques d'accès au médium **CSMA/CA** et **TDMA**. C'est la période **CFP** qui contient les trames des applications les plus contraintes. Pour cette raison, nous avons choisi de calculer les valeurs de **BO** et **SO** selon le temps d'inter-génération le plus petit de l'application la plus contrainte dans la période **CFP**.

Après la proposition d'une solution d'adaptation des valeurs de **BO** et **SO** aux types des trames transmises dans le réseau, nous sommes naturellement passé à l'étape de simulation. Les résultats de nos simulations montrent que lors de l'utilisation des périodes **CAP** et **CFP** simultanément, les performances du réseau en terme de nombre de messages reçus pour la période **CFP** se dégradent.

Après la vérification approfondie de notre modélisation de la norme, de nos améliorations et modélisation de la solution dans le simulateur, et la vérification de la norme, nous avons remarqué que nous sommes face à une lacune, puisque la norme n'a pas pris en compte la possibilité de transmettre dans les deux périodes **CAP** et **CFP** par le même nœud, comme dans notre cas avec la canne. Ayant pris la décision de ne pas effectuer des changements significatifs sur la couche MAC proposée par la norme, nous avons adopté l'utilisation de la primitive *purge* qui nous permet de supprimer une trame de la file de transmission. Bien que cette solution permette de regagner les performances de réseau dans la période **CFP**, nous constatons une légère dégradation de performance dans la période **CAP**. Puisque cette primitive est générée par notre couche de différenciation, nous l'avons enrichie par l'ajout des fonctions qui permettent la conservation d'une copie de la trame envoyée vers la couche MAC. Les résultats de la simulation ont montré l'efficacité de notre méthode lors de l'utilisation de la *purge*.

Ayant des capteurs qui peuvent générer des alertes, l'utilisation des valeurs fixes de **BO** et **SO** ne résout pas la totalité des problèmes. La diversité des applications qui appartiennent à des profils différents peut générer des problèmes si nous choisissons des valeurs de **BO** et **SO** qui ne sont pas adéquates aux besoins des capteurs de la canne qui représentent les applications les plus exigeantes dans le réseau.

Parmi les cas où nous avons besoin de changer la valeur de **BO** et **SO**, se distingue celui du passage d'une canne à un état critique par la génération d'une alerte. Ceci nous a amené à chercher une solution dynamique. Lors de la réception d'une alerte, la couche de différenciation procède à une étape de validation et de recalcul des valeurs de **BO**

et **SO**. Nous avons proposé une relation mathématique entre les valeurs de **BO** et **SO** et les paramètres de taille de la file d'attente, de temps d'inter-génération et de temps nécessaire de transmission. Les équations proposées nous offrent la possibilité de trouver la durée exacte de **BI**, **SD** et la période d'inactivité.

Nous avons également proposé une équation mathématique qui permet l'adaptation des **GTS** réservés en nombre et position de slots avec la nouvelle configuration de la supertrame. Cette solution nous permet d'être plus performant au niveau du temps nécessaire pour l'annulation et la réallocation des slots **GTS**. Les résultats des simulations ont montré que le réseau garde les mêmes performances lors de l'apparition d'un état critique.

La couche de différenciation que nous avons proposée utilise un graphe d'états qui implémente les différentes situations qui peuvent être générées dans un nœud. Nous pouvons voir cette couche comme une extension de la couche MAC qui offre des améliorations et des mécanismes d'adaptation aux besoins des applications temps réel.

Parmi les applications les plus contraintes, nous trouvons la transmission de la voix à travers les couche MAC et physique de la norme 802.15.4. Cette application représente un élément important dans le projet CANet. Une étude sur les **codecs** et sur les meilleures valeurs de **BO** et **SO** a été faite. Suite à cette étude, nous recommandons d'utiliser le codec Opus avec $\text{BO} = \text{SO} = 3$.

Nos travaux sont concentrés essentiellement sur l'architecture du réseau, le choix technologique et la couche différenciation.

Nous n'avons pas retravaillé la période d'association qui représente une étape préliminaire. En effet, dans cette période, le coordinateur doit juste collecter en plus les informations nécessaires pour la couche différenciation afin qu'elle puisse vérifier l'adaptation des paramètres protocolaires aux exigences des applications des nouvelles cannes associées.

La méthode proposée pour donner plus de priorité à la canne qui contient un état critique dans la période **CAP** n'est pas généralisée pour le cas de l'existence de plusieurs cannes en alerte dans le réseau. Cette situation est jugée toutefois assez rare.

Dans toutes les simulations, nous avons supposé que les cannes utilisent les mêmes applications. Cette hypothèse nous permet d'étudier facilement la variation et les performances de notre réseau, puisque nous avons les mêmes paramètres dans chaque application de même type dans le réseau. En réalité, les cannes peuvent éventuellement être équipées par des capteurs différents.

Le nombre maximal d'applications qui peuvent utiliser la période **CFP** se limite à une seule. Cette limite est fixée par la norme puisque le nombre maximal de réservations de **GTS** est égal à 2 **GTS** (1 **GTS** pour la transmission et 1 **GTS** pour la réception) pour chaque nœud.

Perspectives

L'une des principales perspectives de recherche qui apparaissent à l'issue de notre thèse concerne l'amélioration de la couche différenciation par l'ajout de nouvelles fonctionnalités qui permettent la réservation de plusieurs [GTS](#). La couche de différenciation pourrait alors gérer la transmission des trames dans plusieurs GTS virtuels vus comme un seul [GTS](#) au niveau MAC.

La présence de plusieurs types de trafics dans une même canne et sur le réseau nous amène à traiter le cas de l'existence d'un trafic mixte qui appartient à la même file d'attente. La solution qui doit être proposée pour ce problème permet la différenciation entre des trafics qui appartiennent à la même classe de profil selon les besoins du centre de contrôle et de suivi.

Dans notre travail, nous nous sommes concentrés sur la partie de la topologie correspondant aux échanges entre cannes et [CMAP](#). Une étude des communications entre les [CMAP](#) avec la présence des cannes serait une perspective intéressante pour voir les performances générales de toute l'architecture. Cette étude aurait pour objectif de résoudre le problème d'adressage qui semble complexe puisque la norme [IEEE 802.15.4](#) n'est pas faite pour utiliser les adresses IPv4 ou IPv6. La solution proposée devrait prendre en considération la consommation de l'énergie et faciliter l'étape de *Hand-over* entre les [CMAP](#).

L'implémentation réelle de notre solution sera utile pour appréhender les résultats réels et les comparer avec les résultats de simulation, en particulier pour évaluer le temps lié au changement de contexte lors de la prise en compte des nouvelles valeurs de [BO](#) et [SO](#). Un *testbed* réel sera également utile pour toute valorisation ou transfert de technologie vers une pré-industrialisation.

Dans notre thèse, nous avons proposé une couche différenciation qui étend et améliore les fonctionnalités proposées par la couche MAC de 802.15.4, afin de la rendre compatible avec les besoins de tout projet qui utilise plusieurs capteurs en même temps. Cette couche de gestion rend possible l'adaptation aux besoins des applications contraintes comme des applications tolérantes temporellement.

Cette couche contient les fonctions et les méthodes nécessaires qui permettent la manipulation et le suivi des paramètres de la couche MAC sans effectuer le moindre changement de protocole. Il sera intéressant de travailler au niveau de cette couche et de ses fonctionnalités qui pourront être améliorées pour s'adapter à d'autres services.

Enfin, à plus long terme, il serait intéressant d'adapter nos solutions d'architecture, de topologie hybride, et de protocoles, aux nouveaux réseaux dédiés au domaine étudié, tel que le nouveau standard [IEEE 802.15.6](#).

Publications personnelles

Articles de revues internationales

[P1] Sabri Khssibi, Adrien Van den Bossche, Thierry Val, Hanen Idoudi, Leila Azzouz Saidane. Optimization of IEEE 802.15.4: Overview, Theoretical Study and Simulation. Dans : International Journal of Information and Communication Technology, Inderscience Publishers, Vol. 1, octobre 2014.

[P2] Sabri Khssibi, Hanen Idoudi, Adrien Van den Bossche, Thierry Val, Leila Azzouz Saidane. Presentation and analysis of a new technology for low-power wireless sensor network. Dans : International Journal of Digital Information and Wireless Communications, The Society of Digital Information and Wireless Communications (SDIWC), Vol. 3 N. 1, 2013.

Conférences et workshops internationaux

[P3] Sabri Khssibi, Hanen Idoudi, Adrien Van den Bossche, Thierry Val, Leila Azzouz Saidane. Etude et proposition d'un ordonnancement optimisé des slots de temps garantis sur un WPAN 802.15.4 (poster). Dans : International Conference on Sciences of Electronics, Technologies of Information and Telecommunications, Sousse, Tunisie, IEEE, 2012.

[P4] Sabri Khssibi, Hanen Idoudi, Adrien Van den Bossche, Thierry Val, Leila Azzouz Saidane. Overview, Metrology and Theoretical Study on the New WSN Protocol: ANT. Dans : International Workshop on Performance Evaluation and Modeling in Wireless Networks: PEMWN, Tunis, Tunisie, 2012.

Conférences et workshops nationaux

[P5] Sabri Khssibi, Adrien Van den Bossche, Hanen Idoudi, Leila Azzouz Saidane, Thierry Val. Transmission de la voix sur des liens sans fil IEEE 802.15.4. Dans :

Journées Nationales des Communications Terrestres (JNCT 2014), Éditions Universitaires Européennes, Toulouse-Blagnac, France, 2014.

[P6] Sabri Khssibi, Hanen Idoudi, Thierry Val, Adrien Van den Bossche. Classification des techniques d'allocation de GTS de la norme IEEE 802.15.4 et Proposition de Nouvelles Méthodes (regular paper). Dans : Journées Doctorales en Informatique et Réseaux (JDIR 2011), Belfort-Montbéliard, France, 2011.

Bibliographie

- [1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. Wireless sensor networks: A survey. *Computer Networks*, 38(4):393–422, 2002.
- [2] John Stankovic. When sensor and actuator networks cover the world. *ETRI Journal*, 30(5):627–633, 2008.
- [3] Khaldoun Al Agha, Marc-Henri Bertin, Tuan Dang, Alexandre Guitton, Pascale Minet, Thierry Val, and Jean-Baptiste Viollet. Which wireless technology for industrial wireless sensors network? the development of OCARI technology. *IEEE Transactions on Industrial Electronics*, 56(10):13, 2009.
- [4] N. Noury, T. Herve, V. Rialle, G. Virone, E. Mercier, G. Morey, A. Moro, and T. Porcheron. Monitoring behavior in home using a smart fall sensor and position sensors. In *Microtechnologies in Medicine and Biology, 1st Annual International Conference On. 2000*, pages 607–610, 2000.
- [5] Loren Schwiebert, Sandeep K.S. Gupta, and Jennifer Weinmann. Research challenges in wireless networks of biomedical sensors. In *Proceedings of the 7th Annual International Conference on Mobile Computing and Networking, MobiCom '01*, pages 151–165. ACM, 2001. ISBN 1-58113-422-3.
- [6] G. Eysenbach. What is e-health? *Journal of Medical Internet Research*, 3(2):e20, 2001.
- [7] Elizabeth Bougeois, Adrien Van den Bossche, Nicolas Cazenave, Laurence Redon, Adriana Soveja, Thierry Val, and Thierry Villemur. *Le projet CANet : une activité pluridisciplinaire liant recherche et pédagogie (regular paper)*. -, 2012.
- [8] Thierry Val, Elizabeth Bougeois, Adrien Van den Bossche, Nicolas Cazenave, Laurence Redon, Adriana Soveja, and Thierry Villemur. Projet CANet : un système de suivi de personnes à mobilité réduite grâce à leur canne de marche. *Magazine des IUT de France, Recherche*, Hors-série:10–11, 2013.
- [9] <http://www.ubitennis.com/english/2014/04/30/babolat-pure-drive-play-intelligent-racquet-service/>, babolat pure drive play: the intelligent racquet at your service, Vue le 21/06/2014.

- [10] <http://indianexpress.com/article/sports/tennis/intelligent-racquets-to-be-the-new-tool-for-data-mining-in-tennis/>, intelligent racquets to be the new tool for data mining in tennis, Vue le 12/07/2014.
- [11] <http://indianexpress.com/article/sports/tennis/intelligent-racquets-to-be-the-new-tool-for-data-mining-in-tennis/>, intelligent racquets to be the new tool for data mining in tennis, Vue le 12/07/2014.
- [12] <http://esa.un.org/wpp/>, world population prospects: The 2012 revision, Vue le 12/07/2014.
- [13] <http://www.globalaging.org/elderrights/world/2010/ga65fr.pdf>, suite donnée à la deuxième assemblée mondiale sur le vieillissement : examen détaillé, Vue le 18/07/2014.
- [14] <http://ec.europa.eu/programmes/horizon2020/en/h2020-section/health-demographic-change-and-wellbeing>, health, demographic change and wellbeing, Vue le 14/08/2014.
- [15] Blanpain Nathalie and Chardon Olivier. *Projections de population à l'horizon 2060. Un tiers de la population âgé de plus de 60 ans*, volume 1. Insee, 10 edition, 2010.
- [16] Vincenzo Della Mea. What is e-health (2): The death of telemedicine? *Journal of Medical Internet Research*, 3(2):e22, 2001.
- [17] Terrance J.Dishongh and Michael McGrath. *Wireless sensor networks for health-care application*. Artech House, 1 edition, 2009.
- [18] <http://www.neatorama.com/2013/10/27/an-autonomous-self-steering-robot-cane-for-the-blind>, an autonomous, self-steering robot cane for the blind, Vue le 16/08/2014.
- [19] [http://www.silvereco.fr/the-aid% c 2 % a 0 -une-canne-intelligente-pour-personnes-agees-laureate-du-fujitsu-design-award-2011/311620](http://www.silvereco.fr/the-aid%c2%a0-une-canne-intelligente-pour-personnes-agees-laureate-du-fujitsu-design-award-2011/311620), the aid : une canne intelligente pour personnes âgées lauréate du fujitsu design award 2011, Vue le 16/05/2014.
- [20] <http://www.silvereco.fr/la-canne-intelligente-de-fujitsu-du-concept-design-au-prototype/315031>, la canne intelligente de fujitsu : du concept design au prototype, Vue le 16/05/2014.
- [21] http://www.hockeyshot.ca/fwd_powershot_hockey_sensor_p/accessory-061.htm, fwd powershot sensor, Vue le 20/05/2014.
- [22] <http://store-quattrium.com/collections/frontpage/products/fwd-powershot>, fwd powershot, Vue le 20/05/2014.

- [23] <http://indianexpress.com/article/sports/tennis/intelligent-racquets-to-be-the-new-tool-for-data-mining-in-tennis>, intelligent racquets to be the new tool for data mining in tennis, Vue le 21/07/2014.
- [24] <http://www.thisisant.com/>, ANT, Vue le 22/09/2014.
- [25] *IEEE std5802.15.2 : Coexistence of Wireless Personal Area Networks with Other Wireless Devices Operating in Unlicensed Frequency Band*. IEEE802, 2003.
- [26] <http://www.epo.org/learning-events/european-inventor/finalists/2012/haartsen.html>, Bluetooth technology, Vue le 20/07/2014.
- [27] <http://en.hartcomm.org/>, wirelessHART, Vue le 01/01/2015.
- [28] <http://www.bluetooth.com/pages/history-of-bluetooth.aspx>, History of the Bluetooth Special Interest Group, Vue le 20/07/2014.
- [29] *Specification of the Bluetooth System, Covered Core Package, Version: 4.0*. The Bluetooth Special Interest Group: Kirkland, USA, 2010.
- [30] JAAP C. Haartsen. The Bluetooth radio system. *Personal Communications, IEEE*, 7(1):28–36, 2000.
- [31] K. Townsend, C. Cufí, and R. Davidson. *Getting Started with Bluetooth Low Energy: Tools and Techniques for Low-Power Networking*. Oreilly & Associates Incorporated, 2014.
- [32] Carles Gomez, Joaquim Oller, and Josep Paradells. Overview and evaluation of Bluetooth Low Energy: An emerging low-power wireless technology. *Sensors*, 12(9):11734–11753, 2012.
- [33] Omer A. Bamahdi and Salam A. Zummo. An adaptive frequency hopping technique with application to Bluetooth-WLAN coexistence. *Mobile Communications and Learning Technologies, Conference on Networking, Conference on Systems, International Conference on*, 1:131, 2006.
- [34] H. Gan B. Tresier and V. Sapozhnykov. *Non-collaborative AFH Mechanism*. 2001.
- [35] N. Hunn. *Woungang, pervasive computing and network*. Cambridge, USA, 2010.
- [36] Ali Maleki Tabar, Arezou Keshavarz, and Hamid Aghajan. Smart home care network using sensor fusion and distributed vision-based reasoning. In *Proceedings of the 4th ACM International Workshop on Video Surveillance and Sensor Networks, VSSN '06*, pages 145–154, USA, 2006. ACM.
- [37] Technical report, Zigbee alliance, Vue le 22/07/2014.
- [38] <http://fr.hartcomm.org/>, wirelesshart, Vue le 22/07/2014.
- [39] http://cache.freescale.com/files/rf_if/doc/ref_manual/synkrorm.pdf, synkrorc, Vue le 22/07/2014.

- [40] <http://www.smkusa.com/usa/technologies/rf4ce/>, rf4ce, Vue le 22/07/2014.
- [41] ISA100. standard des radiocommunications dans l'industrie, Vue le 22/07/2014.
- [42] 802.15.4-2011. Standard ieee802.15.4, Vue le 22/07/2014.
- [43] K.i. Hwang J. Kim and D.s. Eom. Voice communication using extended concept of GTS in IEEE 802.15.4. *Korea Institute of Communication Summer, General Conference*, 1:482, 2007.
- [44] Alexandre Guitton and Nassima Hadid. Analysis of channel access delay of slotted csma/ca in a wsn. In *Sensor Systems and Software*, volume 24, pages 83–97. Springer Berlin Heidelberg, 2010.
- [45] Mohammad S. Obaidat, Mieso Denko, and Isaac Woungang. *W. Stallings*. Pearson Prentice Hall, USA, 2004.
- [46] Specification of the Bluetooth system. Specification Bluetooth, Vue le 22/07/2014.
- [47] Linqing Gui, Thierry Val, Anne Wei, and Rejane Dalce. Improvement of range-free localization technology by a novel DV-Hop protocol in wireless sensor networks. *Ad Hoc Networks Journal*, 24(Part B):(on line), 2015.
- [48] Rejane Dalce, Adrien Van den Bossche, and Thierry Val. Indoor self-localization in a WSN, based on time of flight: Propositions and demonstrator (regular paper). In *IEEE International Conference on Indoor Positioning and Indoor Navigation (IPIN)*, page (electronic medium). IEEEExplore digital library, 2013.
- [49] <http://standards.ieee.org/>, les standards ieee, Vue le 01/09/2015.
- [50] A. El-Hoiydi and J.-D. Decotignie. WiseMAC: an ultra low power MAC protocol for the downlink of infrastructure wireless sensor networks. In *Computers and Communications, 2004. Proceedings. ISCC 2004. Ninth International Symposium on*, volume 1, pages 244–251, 2004.
- [51] Kyung Sup Kwak, S. Ullah, and N. Ullah. An overview of IEEE 802.15.6 standard. In *Applied Sciences in Biomedical and Communication Technologies (ISABEL), 2010 3rd International Symposium on*, pages 1–6, 2010.
- [52] A. Astrin and al. IEEE p802.15-08-0780-09-0006. IEEE TG6 Draft, 2009.
- [53] M. Hernandez and L. Mucchi. *Body Area Networks using IEEE 802.15.6: Implementing the ultra wide band physical layer*. Academic Press library in Biomedical Application of mobile and wireless Communication, USA, 2014.
- [54] Keränen N., Särestöniemi M., Partala J., Hämäläinen M., Reponen J., Seppänen T., Iinatti J., and Jämsä T. IEEE 802.15.6-based multi-accelerometer WBAN system for monitoring parkinson's disease. In *Proc. 35th Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, pages 1656–9, 2013.

- [55] C. Tachtatzis, F. Di Franco, D.C. Tracey, N.F. Timmons, and J. Morrison. An energy analysis of IEEE 802.15.6 scheduled access modes. In *GLOBECOM Workshops (GCWkshps), 2010 IEEE*, pages 1270–1275, 2010.
- [56] 802.15.6-2012 – IEEE standard for local and metropolitan area networks – part 15.6: Wireless body area networks, 2012.
- [57] Olufemi Ekundayo. *Body Area Network Standardization, Analysis and Application*. Phd, Savonia University Of Applied Sciences, 2013.
- [58] <http://www.thisisant.com>, ant message protocol and usage, application notes, Vue le 23/09/2014.
- [59] <http://www.thisisant.com/>, ant channel search and background scanning channel, application notes, Vue le 23/09/2014.
- [60] <http://www.thisisant.com>, ant message protocol and usage, application notes, Vue le 23/09/2014.
- [61] <http://www.thisisant.com/>, proximity search, application notes, Vue le 23/09/2014.
- [62] G.-Z. Yang. *Body Sensor Networks*. Springer, Britagne, 2014.
- [63] Konstantin Mikhaylov, Nikolaos Plevritakis, and Jouni Tervonen. Performance analysis and comparison of Bluetooth low energy with IEEE 802.15.4 and simplici. *Journal of Sensor and Actuator Networks*, 2(3):589–613, 2013.
- [64] Jin Soo Choi and MengChu Zhou. Performance analysis of ZigBee-based body sensor networks. In *Systems Man and Cybernetics (SMC), 2010 IEEE International Conference on*, pages 2427–2433, 2010.
- [65] C. Links. Bluetooth and ZigBee: a new standards war brewing? page (on line).
- [66] Navrati Saxena, Abhishek Roy, and Jitae Shin. Dynamic duty cycle and adaptive contention window based QoS-MAC protocol for wireless multimedia sensor networks. *Computer Networks*, 52(13):2532 – 2542, 2008.
- [67] A.M. Firoze, L.Y. Ju, and L.M. Kwong. PR-MAC a priority reservation MAC protocol for wireless sensor networks. In *Electrical Engineering, 2007. ICEE '07. International Conference on*, pages 1–6, 2007.
- [68] Priority-based service differentiation scheme for IEEE 802.15.4 sensor networks. *AEU - International Journal of Electronics and Communications*, 61(2):69 – 81, 2007.
- [69] Tae Hyun Kim and Sunghyun Choi. Priority-based delay mitigation for event-monitoring IEEE 802.15.4 LR-WPANs. *Communications Letters, IEEE*, 10(3): 213–215, 2006.

- [70] Yang Liu, I. Elhanany, and Hairong Qi. An energy-efficient QoS-aware media access control protocol for wireless sensor networks. In *Mobile Adhoc and Sensor Systems Conference, 2005. IEEE International Conference on*, pages 191–194, 2005.
- [71] Yu-Kai Huang, Ai-Chun Pang, and Hui-Nien Hung. An adaptive GTS allocation scheme for IEEE 802.15.4. *Parallel and Distributed Systems, IEEE Transactions on*, 19(5):641–651, May 2008.
- [72] Demosthenes Vouyioukas, Ilias Maglogiannis, and Dimitris Komnakos. Emergency m-health services through high-speed 3G systems: Simulation and performance evaluation. *Simulation : Transactions of The Society for Modeling and Simulation International*, 83(4):329–345, 2007.
- [73] Tan-Hsu Tan, M. Gochoo, S. Bilgee, Ching-Su Chang, Jin-Jia Hu, Yung-Fu Chen, J.Y. Chiang, Yung-Fa Huang, Ming-Hui Lee, Yung-Nian Hsu, and Jin-Chyr Hsu. Development of an emergency medical service system based on wireless networks and real-time traffic information. In *International Conference on Computerized Healthcare (ICCH)*, pages 35–42, 2012.
- [74] Javier Pindter Medina, Javier Eduardo Gonzalez Villarruel, and Blanca Tovar Corona. Proposal for an m-health system. In *Electronics, Robotics and Automotive Mechanics Conference*, pages 55–59, 2009.
- [75] Lea Skorin-Kapov and Maja Matijasevic. Analysis of QoS requirements for e-Health services and mapping to evolved packet system QoS classes. *Int. J. Telemedicine Appl.*, 1:9:1–9:18, 2010.
- [76] S. khssibi, T. Val, H. Idoudi, and A. V. D. Bossche. Classification des techniques d’allocation de GTS de la norme IEEE 802.15.4 et proposition de nouvelles méthodes. In *Journées Doctorales en Informatique et Réseaux*, 2011.
- [77] <http://www.fmcoeur.com>, signes d’une crise cardiaque, d’un arrêt cardiaque et du syndrome de la mort subite par arythmie, Vue le 15/01/2015.
- [78] Rejane Dalce, Thierry Val, and Adrien Van den Bossche. Comparison of Indoor Localization Systems based on Wireless Communications. *Wireless Engineering and Technology*, 2 No 4:(on line), 2011.
- [79] Rejane Dalce, Adrien Van den Bossche, and Thierry Val. Indoor Self-Localization in a WSN, based on Time Of Flight: Propositions and Demonstrator (regular paper). In *IEEE International Conference on Indoor Positioning and Indoor Navigation (IPIN), Montbelliard, 28/10/2013-31/10/2013*. IEEEExplore digital library, 2013.
- [80] Linqing Gui, Thierry Val, Anne Wei, and Rejane Dalce. Improvement of Range-free Localization Technology by a Novel DV-hop Protocol in Wireless Sensor Networks. *Ad Hoc Networks Journal*, 24(Part B):(on line), 2015.

- [81] Sabri Khssibi, Hanen Idoudi, Adrien Van den Bossche, Thierry Val, and Leila Azzouz Saidane. Presentation and analysis of a new technology for low-power wireless sensor network. *International Journal of Digital Information and Wireless Communications*, 3(1):(on line), 2013.
- [82] Hend Fourati and Hanen Idoudi. IEEE802.15.6 standard : General overview. *PEMWN 2014*, 2014.
- [83] Projet DGRS-CNRS (ref : 11/r 14-01): Architectures de communication basées sur les réseaux de capteurs pour la surveillance de personnes (ACOCASP), 2011 - 2013. Equipe RAMSIS, ENSI - Equipe IRT, IRIT, University of Toulouse le Mirail.
- [84] Chiraz Houaidia, Hanen Idoudi, Adrien van den Bossche, Thierry Val, and Leila Azouz Saïdane. Towards an optimised traffic-aware routing in wireless mesh networks. *IJSSC*, 4(3/4):217–232, 2014.
- [85] Chiraz Houaidia, Adrien Van den Bossche, Hanen Idoudi, Thierry Val, and Leila Azzouz Saidane. Impact des interférences dans un réseau sans fil multi-sauts (regular paper). In *Journées Nationales des Communications Terrestres (JNCT), Toulouse-Blagnac, 22/05/2014-23/05/2014*, page (support électronique). Éditions Universitaires Européennes, 2014.
- [86] Asma Ben Hadj Mohamed, Thierry Val, Laurent Andrieux, and Abdennaceur Kachouri. Interconnexion d’un réseau IP et d’un réseau domotique KNX pour l’aide au maintien à domicile intelligent (short paper). In *Journées Nationales des Communications Terrestres (JNCT), Toulouse-Blagnac, 22/05/2014-23/05/2014*, page (support électronique). Éditions Universitaires Européennes, 2014.
- [87] Aggeliki Sgora, Dimitrios D. Vergados, and Periklis Chatzimisios. IEEE 802.11s wireless mesh networks: Challenges and perspectives. In Fabrizio Granelli, Charalabos Skianis, Periklis Chatzimisios, Yang Xiao, and Simone Redana, editors, *MOBILIGHT*, volume 13, pages 263–271. Springer, 2009.
- [88] P. Jacquet, P. Muhlethaler, T. Clausen, A. Laouiti, A. Qayyum, and L. Viennot. Optimized link state routing protocol for ad hoc networks. In *Multi Topic Conference, 2001. IEEE INMIC 2001. Technology for the 21st Century. Proceedings. IEEE International*, pages 62–68, 2001.
- [89] D. Skordoulis, Qiang Ni, Hsiao-Hwa Chen, A.P. Stephens, Changwen Liu, and A. Jamalipour. IEEE 802.11n MAC frame aggregation mechanisms for next-generation high-throughput WLANs. *Wireless Communications, IEEE*, 15(1): 40–47, 2008.
- [90] Lieven Tytgat, Opher Yaron, Sofie Pollin, Ingrid Moerman, and Piet Demeester. Avoiding collisions between IEEE 802.11 and IEEE 802.15.4 through coexistence aware clear channel assessment. *Eurasip Journal on Wireless Communication and Networking*, pages 137:1–137:15, 2012.

- [91] Wei Yuan, Xiangyu Wang, Jean-Paul M. Linnartz, and Ignas G. Niemegeers. Coexistence performance of IEEE 802.15.4 wireless sensor networks under IEEE 802.11b/g interference. *Wirel. Pers. Commun.*, 68(2):281–302, 2013. ISSN 0929-6212.
- [92] Wei Yuan, Xiangyu Wang, Jean-Paul M. G. Linnartz, and Ignas G. Niemegeers. Experimental validation of a coexistence model of IEEE 802.15.4 and IEEE 802.11b/g networks. *IJDSN*, 1, 2010.
- [93] NPX, co-existence of IEEE 802.15.4 at 2.4 GHz application note,. Disponible sur [http : //www.nxp.com/documents/application_note/JN – AN – 1079.pdf](http://www.nxp.com/documents/application_note/JN-AN-1079.pdf), . Vue le 19/02/2014.
- [94] Nezo Ibrahim Fofana, Adrien Van den Bossche, and Thierry Val. Étude des couches MAC dédiées à l’UWB (short paper). In *Journées Nationales des Communications Terrestres (JNCT), Toulouse-Blagnac, 22/05/2014-23/05/2014*, page (en ligne). Éditions Universitaires Européennes, 2014.
- [95] www.speex.org, site web officiel de speex, . Vue le 12/03/2014.
- [96] www.ilbcfreeware.org, site web officielle de ilbc, . Vue le 06/04/2014.
- [97] www.voip-sip.org/voip-codec-payload-bandwidth-required, présente des informations sur des différentes codecs voip, . Vue le 12/03/2014.
- [98] Anssi Rämö and Henri Toukoma. Voice quality characterization of IETF opus codec. In *INTERSPEECH 2011, 12th Annual Conference of the International Speech Communication Association, Florence, Italy, August 27-31, 2011*, pages 2541–2544, 2011.
- [99] Itu-t recommendation g.114 – one-way transmission time.itu-t. In *International Telecommunication Union*, 2003.
- [100] <http://www.lextronic.fr/r2484-microcontroleur-jn5148.html>, site web de officielle de lextronic, . Vue le 12/05/2014.
- [101] opus-codec.org/comparaison/googletest2.pdf, les tests effectués par google sur les codecs opus, ilbc, speex, etc., . Vue le 12/03/2014.
- [102] <https://omnetpp.org/>, cite officiel de omnet, Vue le 10/04/2015.
- [103] Yunjiao Xue, Ho Sung Lee, Ming Yang, P. Kumarawadu, H.H. Ghenniwa, and Weiming Shen. Performance evaluation of ns-2 simulator for wireless sensor networks. In *Canadian Conference on Electrical and Computer Engineering (CCECE)*, pages 1372–1375, 2007.
- [104] <https://inet.omnetpp.org/>, inet plateforme, Vue le 01/01/2015.
- [105] <https://github.com/aarizaq/inetmanet-2.0>, inetmanet plateforme, Vue le 02/08/2014.

-
- [106] Atta ur Rehman Khan, Sardar Muhammad Bilal, and Mazliza Othman. A performance comparison of network simulators for wireless networks. *CoRR*, 1, 2013.